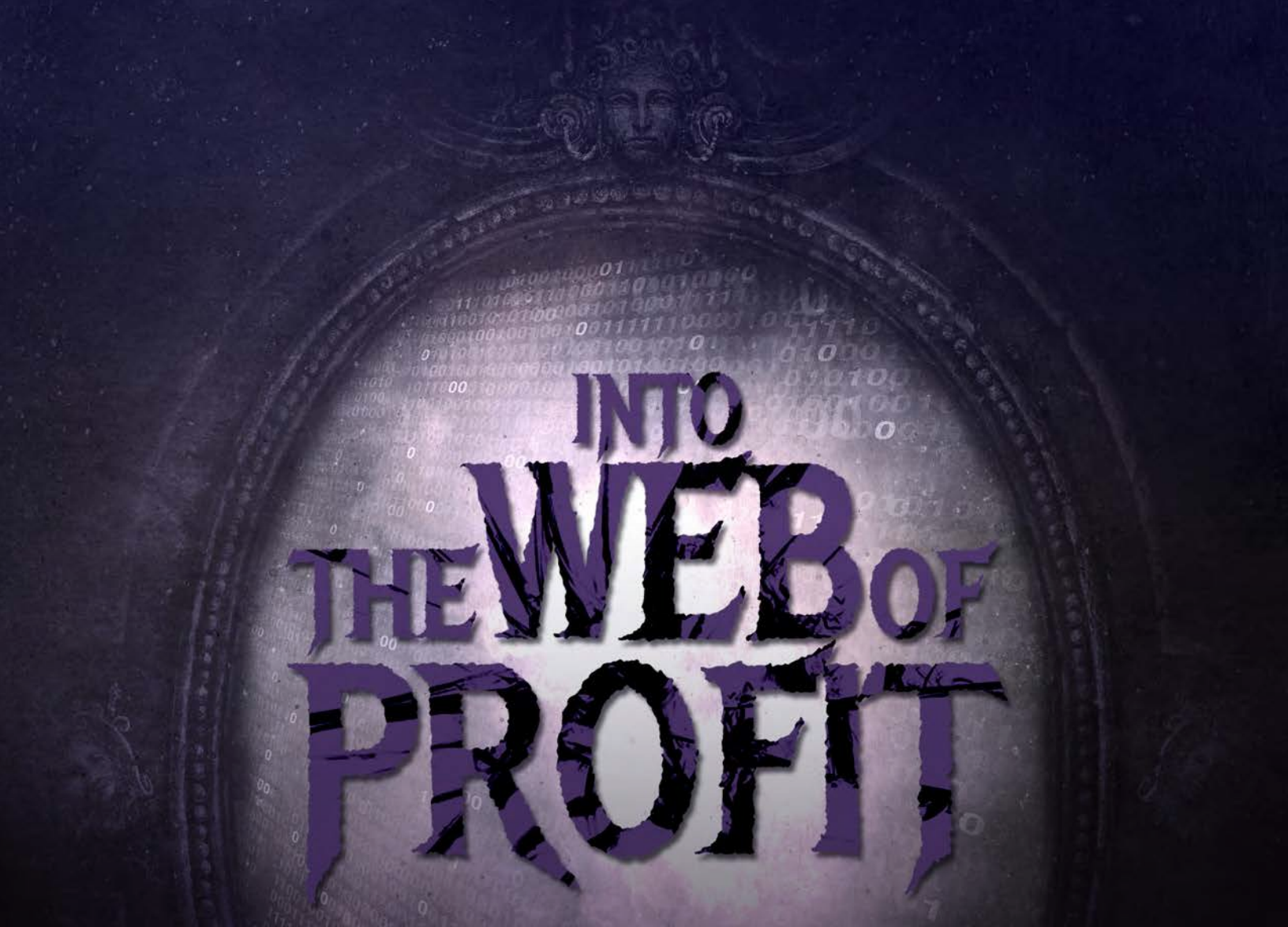


ダークネットの暗い鏡の向こう側
企業に対する脅威

Into The Web of Profit の次の章

犯罪学上級講師
Michael McGuire博士
Surrey大学

内容

序文

GREGORY WEBB
CEO of Bromium

McGuire博士と一緒に仕事をするといつも目が覚めるような発見があり、その学術的研究は、私たちが長年疑ってきたことを裏付けるものです。サイバー犯罪は悪者にとって信じられないほど儲かるビジネスで、企業も政府も自分たちの身を守るために十分なことをしていないのです。私たちが2018年に発表した最初のレポート 'Into the Web of Profit' [1] では、サイバー犯罪経済が毎年1.5兆ドルもの莫大な収益を生み出していることが明らかになりました - この数字は今後も増加し続ける可能性が高く、その資金の一部は、人身売買やテロリズムを含む従来の犯罪に再投資されています。

しかし、この報告書の中で最も興味深い、そしておそらく予想外の発想は、サイバーを利用した犯罪の新たな形態であるプラットフォーム犯罪を明らかにしたことです。サイバー犯罪者は、データが一番の商品となる、UberやAmazonなどが利用している破壊的なプラットフォームベースのビジネスモデルを真似ています。クリアウェブは良いものですが、その鏡像は悪質で規制が無く危険なものです。

このレポートでは、McGuire博士がダークネットの覗き窓から、プラットフォーム犯罪がどのように企業を標的とした新しいサービスの波を呼び起こしているかを検証しています。McGuire博士の調査結果はダークウェブに光を当てています。ダークウェブは、IPやデータの窃盗、秘密の取引、業務の混乱、企業のスパイを狙うサイバー犯罪者にとっては、まさに駄菓子屋のような場所です。

レンタル・ハッカーはビジネスです。彼らは組織に潜入し、洗練されたネットワークを構築し、企業全体を不安定化させ、カスタマイズされたマルウェアを作成します。今回の調査では、今日のサイバー犯罪者が目的達成のためにどれほどの決意を持っているかが明らかになり、個人や企業を騙すために使用する手法や技術に光が当てられました。

ダークネット・サービスがますますオーダーメイドでターゲットを絞った性質を持っていることは、競争力や収益の保護から評判や事業の継続性に至るまで、ビジネスにとっての重大なリスクであることに警鐘を鳴らすものです。露骨で、リスクが高く、心配な傾向が企業をせきたてています。

1. **カスタムマルウェアは売り手市場です：**カスタムマルウェアの需要は、ゼロデイ、ポリモーフィックマルウェア、特定の業界に合わせたマルウェアの需要が増加しており、「既製品」バージョンを2:1で上回りました。これは、検知ベースのセキュリティツールが知らないカスタマイズされた脅威が、企業のIT資産をいつでも攻撃し、いとも簡単に防御を切り裂く可能性があることを意味しています。
2. **ビジネスへのターゲットを絞ったアクセス：**多くのベンダーが個別企業へのアクセスを提供しており、その60%以上が10以上の企業ネットワークへのゲートウェイを提供し、金融サービスや医療機関が最も人気があります。また、社内にデジタルで保存されている企業データやその他の貴重なIPを取得しようとするスパイサービスも提供しています。
3. **フィッシングと連動したなりすまし：**eBay、Amazon、Minecraftなどの安価ななりすましページから、40ドルのフルサービスのフィッシング・キットまで、ダークネットの利用者は、大量のフィッシングキャンペーンで企業をターゲットにするために必要なものをすべて購入することができます。さらに問題なのは、悪意のない従業員を騙して悪意のある実行ファイルを起動させるために使用される請求書やその他の公式文書がすぐに入手できることです。

民間や政府の組織が2017年から20212年にかけてサイバーセキュリティ製品やサービスに累積的に支出すると予想される金額は1兆ドルを超えるにもかかわらず、サイバー犯罪の量は非常

[1] Into the Web of Profit, April 2018年

に膨大で、史上最大かつ最速の富の移動とも言われています。[2] 私たちは、より良い方法で対策を講じることができます。サイバー犯罪者は常に企業のセキュリティ対策の一歩先を行っているように見え、ダークネット・プラットフォームの普及により、ますますそれが容易になっています。ダークネット上の脅威がもたらすリスクを十分に理解することで、サイバー犯罪者の戦術に対抗し、そのネットワークを破壊することができます。しかし、そのためには、企業はセキュリティを全面的に見直し、検知を超えた多層的な防御策を展開することによってのみ、合法的なビジネスが状況を変化させることができます。そうしなければ、脅威の潮目を止めること、あるいはダークネット上で秘密やビジネスクリティカルなデータが売買されるのを食い止めることができません。

[2] Cybersecurity Ventures 2017年、 https://cybersecurityventures.com/cybersecurity-market-report/

エグゼクティブサマリー

Michael McGuire博士
Surrey大学 上級講師

ダークネットまたはダーク・ウェブ（以下、本レポートでは「ダークネット」）は、サイバー犯罪が最も活発に行われているドメインの1つとして、不吉な評判を得ています。[3] しかし、デジタル犯罪を助長する役割については広く議論されていますが、企業への影響についてはあまり精査されていません。

本レポートでは、企業とダークネットの関係がどのように進展しているかを、ポジティブな面とネガティブな面の両面から、特に以下の点について考察しています。

(i) ダークネットが企業にもたらす犯罪リスクとその他の課題。

(ii) 「グレーネット」と企業がその資源を利用する際に時として法の限界を超えてどのように活動しているか。

(iii) ダークネットが組織に提供する新たな機会と、これらの機会を活用するために必要な予防策の種類。

このレポートのために、私たちは研究者をダークネットのゲート内およびプライベートのプラットフォームとコミュニティに送り込みました。これにより、サイバー犯罪者がどのように企業をターゲットにしているかについてのユニークな洞察を得ることができ、サイバー犯罪サービスの「ベンダー」とのやり取りを明らかにすることができました。この調査では、ダークネット上で提供されている広告やサービスの例、30人以上のサイバー犯罪者へのインタビュー、法執行機関、セキュリティ専門家、その他のサードパーティの専門家を含むグローバルな専門家パネルからの洞察も紹介しています。

「ダークネット」という言葉は「ダーク・ウェブ」と同じ意味でつかわれています。これは、Google Chromeなどの標準ブラウザではアクセスできません（「クリアネット」と呼ばれることもあります）が、ダークネットに特化した検索エンジンからアクセスできるオンラインコンテンツを指します。

マルウェア、リモートアクセス・トロイの木馬（RAT）、フィッシングなどの企業ネットワークの混乱とアクセスの提供する従来の犯罪対策サービスから、企業スパイ、インサイダー取引、内部告発者のブラックリスト化など、より破壊的な形で影響力を行使するサービスまで、ダークネットが企業に対する脅威を増大させていることは明らかです。また、企業を標的とした攻撃のための特殊なツールや情報の市場も拡大しています。企業内の個々のターゲットにカスタマイズした攻撃の需要が高まっており、ハッカーは財務状況やセキュリティシステム、さらには社内の製品マニュアルなど、あらゆる情報を提供しています。もう一つの重要な発見は、招待制のプラットフォームやプライベートなフォーラムとメッセージング・ネットワークなど、メンバー間のやりとりが法の執行から守られている「インビジブル・ネット」へのシフトです。実際、ダークネットのサービスプロバイダの70%は、暗号化されたプライベートなチャンネルで話をする「インビジブル・ネット」に潜入調査員を招待しています。このため、法の執行機関がダークネット取引を追跡することも、企業が自衛することも、これまで以上に困難になっています。ほとんどの企業は、急速に変化する攻撃経路に対応する準備ができておらず、多くの場合には現在のセキュリティとポリシーが脅威の増大に対処するには不十分です。最終的には、ダークネットがもたらすリスクに対処するためのより強固なシステムを構築するために、企業にとっての脅威の源であると同時に、サイバー犯罪を可能にするものでもあるダークネットについてのより詳細な検討が必要です。

[3] 「ダークネット」という言葉は「ダーク・ウェブ」と同じ意味でつかわれています。これは、Google Chromeなどの標準ブラウザではアクセスできません（「クリアネット」と呼ばれることもあります）が、ダークネットに特化した検索エンジンからアクセスできるオンラインコンテンツを指します。ダークネットは通常、ディープネット/ディープウェブと区別されます。ディープウェブとは、インターネットの他の部分に直接接続されていませんが、特定のパスワードやその他の認証情報を使用してのみアクセスできるオンラインコンテンツを指し、例えば、政府のデータベース、図書館のカタログ、商用イントラネットなどのことです。

数字は語る

- 2016年と比較して、企業に被害をもたらす可能性のあるダークネットのリストの数が20%増加していることがわかりました。これには、標的型マルウェアの販売、特定の企業向けのDDoSサービス、企業データの販売、ブランド偽装フィッシング・ツールの増加などが含まれます。
- 調査員が関与したベンダーの70%が、「インビジブル・ネット」の中でのプライベートチャネルを介した会話に誘導しました。
- 分析されたリストの60%（医薬品を除く）は、企業への直接的な被害の機会を示していました。 ネットワークの侵害、オンラインサービスの停止、または財務上の損失など、即時かつ具体的な損害を引き起こす可能性がありました。
- リストの15%は、ブランドの希薄化や風評被害など、より長期的で抽象的な損害を含む、企業に間接的な損害を与える機会を示していました。さらにリストの25%は、模倣品など、直接的な被害と間接的な被害の両方を引き起こす可能性のある商品を含んでいました。
- 分析されたリストの3分の2はリモート・アクセスによるネットワーク、財務、データを侵害するツールやサービスなどの高い脅威レベルと特徴づけられ、残りは返金詐欺など中程度に分類されています。

ネットワークの侵害

- マルウェア、DDoS、RATは、ダークネット上で利用可能なネットワーク侵害サービスの中で最も一般的なタイプで、ネットワーク侵害に関連する全リストのうち、それぞれ25%、20%、17%を占めています。
- ネットワークアクセスに関連して質問したベンダーのうち、少なくとも60%のベンダーが10以上の企業ネットワークへのアクセスを提供しており、30%が5 ~ 10の間、10%が5つまでのアクセスを提供していました。
- リモート・アクセスの認証情報は、それぞれ2 ~ 30ドルで販売されていました。
- 企業への標的型攻撃の購入費用が平均約4,500ドルであったのに対し、個人への標的型攻撃は2,000ドルでした。
- 発見された最も高価なマルウェアは1,500ドルで、ATMを標的にしたものでした。
- 調査員がFTSE100またはフォーチュン500の企業を対象としてダークネットのハッキングサービスに依頼したところ、約40%から肯定的な回答を得ました。価格は企業によって異なりますが、150ドル ~ 10,000ドルでした。

金銭的な侵害

- 認証情報、フィッシング、返金を得るための偽の領収書は経済的な侵害に関連して提供されたサービスの中で最も一般的なタイプで、リストのそれぞれ38%、27%、14%でした。
- フィッシングに適したページがわずか0.99ドルで販売されており、フルサービスのフィッシング・キットが40ドルから販売されてました。返金に利用できる偽のAmazonの領収書や請求書が52ドルという低価格で販売されていたことが判明しました。

データの侵害

- 消費者口座の詳細、銀行のログイン、および企業の電子メールアドレスは、調査員が発見したデータ漏洩の最も一般的なタイプであり、分析したこのサブセットの28%、21%、および15%をそれぞれ占めていました。
- スパイ活動のサービス（CEOへのアクセスなど）は、1,000ドル ~ 15,000ドルの料金で研究者に提示されました。調査員はまた、インサイダー取引のヒントを提供する複数の個人と接触しました。

イントロダクション

雲をつかむ – 増え続けるインビジブル・ネットへの航海の挑戦

ダークネットの中で道を見つけるのは、濃い霧の中で鏡のホールに入ったような気分になることがよくあります。Googleのような馴染みのある検索エンジンではアクセスできないだけでなく、法執行機関の妨害により、サイトがあっという間に消えてしまうこともあります。しかしながら、このような取り締まりはダークネット取引を終わらせるものではなく、単に一時的に混乱させるだけです。例えば、Silk RoadやAlphaBayがテイクダウンされた後、すぐにその新しいバージョンやクローンが開設されました。レポート[4]よると、そのようなダークネット・プラットフォームのリストは翌週には最大28%増加し、他の多くの知名度の低いサイトもアクティブな状態を維持していました。

ダークネットは普及しているだけでなく、ますます秘密主義的になっています。私たちがやり取りしたベンダーの70%以上が、プライベートなチャネルで話をするよう求めてきたか、既にプライベートまたは暗号化されたメッセージングシステムのみで営業しているかのどちらかでした。このような「見えないネット」を使ったオンライン上でのやり取りの発展は、さらに新しい隠れた形態のサイバー犯罪の出現を支えています。これらの犯罪は、クリアネットとダークネットそれぞれの犯罪と併存し、最終的にはそれを上回る可能性さえあります。これは企業にとっても、研究者や法執行機関にとっても、ダークネットの活動がさらに地下に潜ることになり、憂慮すべき意味を持っています。ダークネットは、多くの組織がそれに対する準備ができておらず、敵対者がデータを盗み、ビジネスを妨害するために必要なあらゆるツールとスキルを備えることを可能にするために、企業にとって大きなリスクです。

1. ダークネット経済-プラットフォーム、商品、利益

クリアネットと同様に、プラットフォームはダークネット上での取引の流れの中心となっています。ダークネットが薬物販売の天国であるという評価は正当なものですが、今回の調査結果は、企業がダークネット上でさまざまな脅威にさらされていることを示唆しています。実際、利用可能なダークネット・プラットフォームのアーカイブ[5]を利用して、2016年の類似のリストと比較すると、企業に対する潜在的な脅威を含むリストが約20%増加していると推定しています。これには、標的型マルウェア、特定企業向けのDDoSサービス、企業データの販売、ブランドを詐称するフィッシング・ツールの増加が含まれます。
この調査で検証された70,000件以上のリスト[6]うち、47% は薬物や薬物関連の販売に関連しており、半数弱 (43%) は、漏洩した銀行口座、マルウェア、DDoS ツール、盗難されたカード認証情報などのデジタル商品関連でした。6%はハッキングチュートリアルなどの「サービス」に関するもので、約4%はその他のものでした。薬物販売に関連するコンテンツを除くと、以下のことがわかりました。

- 60%のダークネット上で取引されているデジタル商品やサービスが企業に直接的な危害を与える可能性があることを示していました。
- 15%のコンテンツが企業に対するより間接的な被害（風評被害など）と関連していました。
- 残りのコンテンツ（全体の約25%）には、偽造品などのアイテムが含まれていました。違法であり、長期的にはブランドの希釈化という点でダメージを与える可能性がありますが、このようなコンテンツは企業にとって当面の関心事ではありませんでした。

ダークネットから企業にもたらされる脅威が重要でかつ上昇していることは明らかです。

---

[4] Kelion （2017年）
[5] 更なる情報はBranwen （2019年）
[6] リストと評価したプラットフォームの詳細は方法論を参照

1.2 – ダークネットが企業にもたらす多面的なリスク - 3次元の脅威評価

これら犯罪の脅威が企業にとってどのような意味を持つのかをより具体的に把握し、その多面的な性質をよりよく理解するために、我々は企業のネットワーク、財務、データを侵害する可能性のあるダークネットツールやサービスの12のカテゴリーから、企業への潜在的な損害を測定する3Dダークネット脅威評価ツール[7]を開発しました。これらの 12 のカテゴリーには以下のものが含まれます。

- 感染/攻撃（マルウェア、DDoS、ボットネットを含む）
- アクセス（RAT、キーロガー、エクスプロイトを含む）
- スパイ活動（サービス、カスタマイズ、標的型攻撃を含む）
- サポートサービス（チュートリアルなど）
- 認証情報
- フィッシング
- 返金
- 顧客データ
- データ
- 財務データ
- IP/営業秘密
- その他の新たな脅威

この12種類の攻撃経路による被害は、専門家パネルによって分析されました。専門家パネルは、各グループのダークネットツールの例を見て、3つの重要な変数について0から30までのスコアを付け、企業に与えうる総合的な影響のレベルを決定しました。これらの変数は次のとおりです。

1. **企業の価値を下げる**：例えば、ブランドの信頼を傷つける、地位および評判の損失、または競争相手に利点を渡すこと
2. **企業を破壊する**：例えば、DDoS攻撃やその他のマルウェアなど、業務の運用に破壊をもたらすもの。
3. **企業を詐取する**：例えば、企業の競争力に影響を与えたり、直接的な財務上の損失をもたらしたりするデータやIPの窃盗やスパイ行為。

その結果（次からのセクションで詳述します）は興味深いものです。分析された12の脅威カテゴリーのうち8つのカテゴリーで、企業は**高**レベルの脅威に直面しています。残りの 4 つのカテゴリーでは**中**レベルの脅威があり、脅威のレベルが低い、または無視できるレベルであることを示すカテゴリーはありません。

あるカテゴリーが企業にとって高レベルの脅威となった場合、それは、破壊する、価値を下げる、または搾取するのいずれかによる損害の可能性が深刻であり、企業全体の現在な実行可能性と長期的な持続可能性に重大なリスクをもたらすと評価されたことを意味します。一方、中程度の脅威は、有害ではあっても、企業の業務継続能力にリスクをもたらす可能性は低いものでした。

[7] このツールがどのように開発されたかの詳細については、方法論を参照してください。

脅威はカテゴリー毎に1 ~ 10点で評価され、合計**30**点満点で評価されます。スコアと脅威のレベルの関係は以下のとおりです。

20 – 30：高い脅威レベル

10 – 19：中程度の脅威レベル

0 – 9：低い脅威レベル

1.3 – 企業ネットワークの侵害を可能にするために販売されているツールやサービス

私たちは、ダークネット・プラットフォームで取引されている企業ネットワークを侵害する可能性のある商品について、4つの大きなカテゴリーを調査しました。これらは、各カテゴリー内の代表的なアイテム、各カテゴリーのアイテム占有率の平均値[8]、アイテムの平均価格、およびカテゴリー全体の3Dエンタープライズ脅威評価[9]とともに、下の表に示されています。

カテゴリー	アイテム	平均 %	平均 価格 $	3D 脅威 スコア	3D 脅威 レベル
ネットワーク侵害					
感染 / 攻撃ツール	マルウェア/ マルウェアサービス	25	3-40	22	高
	DDoS/ボットネット	20	20		
アクセス	RAT	17	2-30	27	高
	エクスプロイト	7	100+		
	キーロガー	6	5		
標的型攻撃とスパイ活動	標的型攻撃サービス	9	15-50+	26	高
サポートサービス	チュートリアル	12	6	18	中
その他	-	4	-		評価無し

表1：ダークネット上のネットワーク侵害ツールとサービス

1.3.1 感染/攻撃ツール

私たちは、企業ネットワークへの感染や攻撃を可能にする様々なツールやサービスを調査しました。フォーラムでの議論を分析し、ベンダーやハッキング・サービスプロバイダからのフィードバックと関連付けることで、企業を標的にするために最も頻繁に使用されるツールの種類を特定することができました。驚くことではありませんが、マルウェアとDDoS/ボットネットのツールは、ネットワーク侵害に関連したダークネットからの脅威の中で最も頻繁に使用されており、調査したリストの平均約45%を占めています(マルウェアが25%、DDoSが20%)。

この研究では、ダークネット上で発見されたいくつかのマルウェアの破壊力が増加しているという懸念すべき傾向が明らかになりました。例えば、Nukeマルウェア[10]は、リモートデスクトップセッションを開き、ターゲットシステムで見つかったライバルのマルウェアをすべて破壊することができます。これにより、犯罪者はマシンを乗っ取り、他のマルウェアを無効にし、マシンをほぼ完全に制御することができます。

[8] 各ドメインを100%として扱い、ダークネット・プラットフォームにある他のアイテムを除外して算出。医薬品はどのカテゴリーにも含まれていませんが、これは販売量が多く、各カテゴリー内での微妙な変化が不明瞭になる可能性があるためです。

[9] 3D 脅威アセスメントのスコアは、本レポートの方法論のセクションに記載されています。

[10] Darkweb news （2017年）

企業にとってより心配なのは、多くの種類のWindowsファイアウォールを回避できることです。この種のウイルスが販売されている例がいくつか見つかりました。特にロシア語のフォーラムでは、企業ネットワークに対する理想的な攻撃ツールとして宣伝されていました。

また、攻撃の実装やマルウェアの管理に、新たな検知困難な経路を利用していることも確認されました。例えば、DDoSのC&Cを隠すためにダークネット上にシフトしたり、インビジブル・ネットの仕組みを利用して、スマートフォンとメッセージングアプリTelegramだけでウェブサイトに潜在するSQLインジェクションの脆弱性をスキャンできるKatyusha Scannerなどのソフトウェアを管理したりすることが挙げられます。これにより、ビジネスインサイダーがスマートフォンだけを使って「現場で」攻撃を受けるリスクも高まります。

また、調査はダークネット上で取引されている感染/攻撃ツールの標的にされる頻度が高い業種を特定することも行いました。その内訳は、以下の表2で見ることができます。最も標的とされている業種として銀行とEコマースがあげられ、医療と教育分野がそれに続いています。

最も頻繁に標的とされる業種

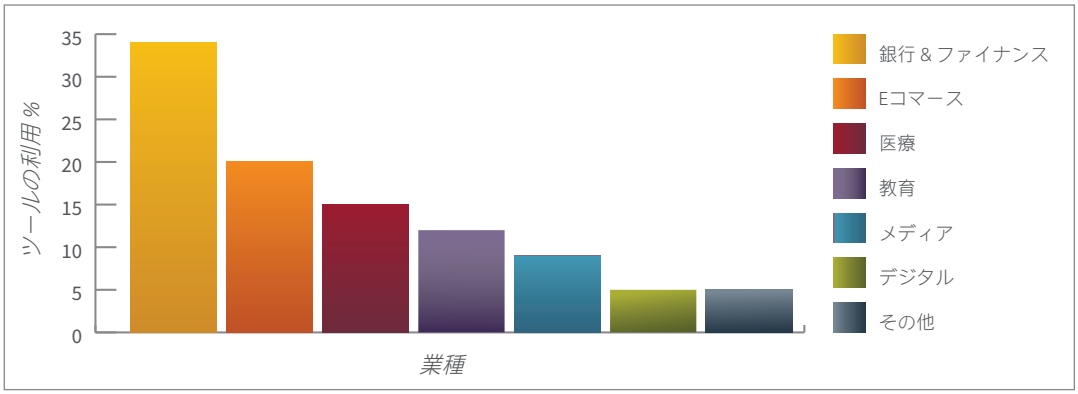


表2：ダークネット感染/攻撃ツールの標的にされることが多い業種

1.3.2 アクセス

私たちが調査したすべてのダークネット市場で、ベンダーが特定の企業ネットワークにアクセスする方法を提供していました。その方法はさまざまで、IT管理者の認証情報を盗むものもあれば、RATのようなマルウェアを提供するものもありました。私たちの研究者は、ネットワークへの「バックドア」を提示されたこともありましたが、これらの詳細については、多額の契約金が支払われるまでは拒否されました。質問したベンダーの少なくとも**60%は**10以上のビジネスネットワークへのアクセスを提供しており、**30%**は5～10のネットワークへのアクセスを提供しており、**10%**は5つのネットワークまでのアクセスを提供していました。

また、企業への攻撃により適合するようなマルウェアの改良も見られました。例えば、クレジットカード情報を盗むために設計されたAZORultマルウェアのようなRATのアップグレードでは、購入者がよりユーザーフレンドリーな管理コントロールパネルを利用できるようになり、多くの企業が利用している検知システムを回避するのに適合するように、アンチウイルスの検知率も低下しています。

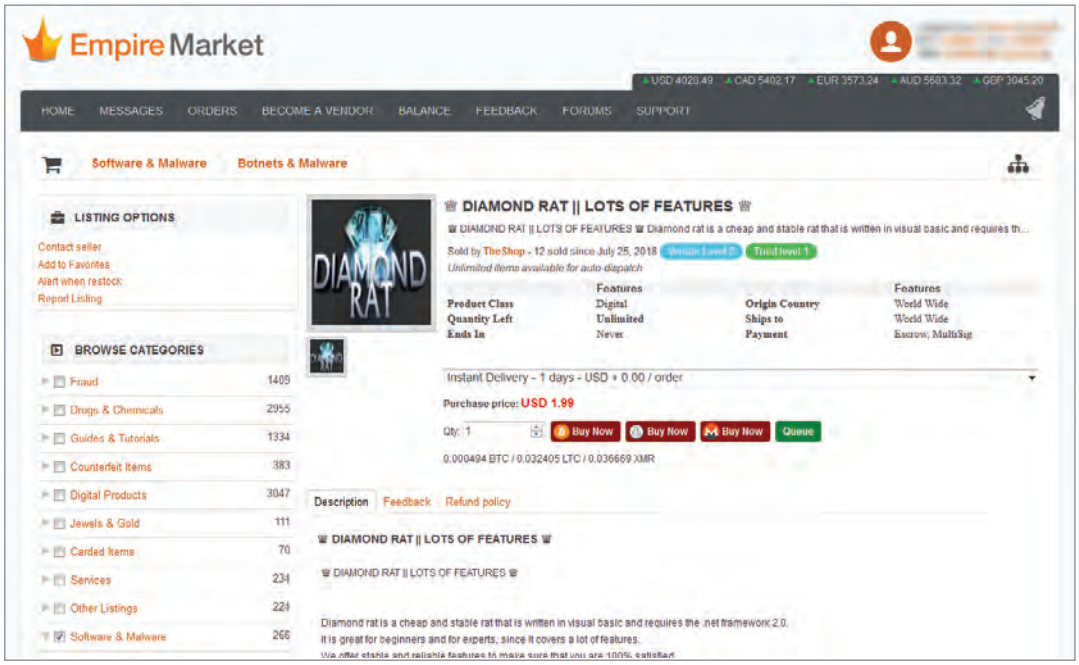
[11] Infosec （2018年）

しかしながら、ますます一般的になってきているアクセスの取得方法は、マルウェアではありません。ネットワーク上のリモートコンピュータを管理するために、Microsoftのプロトコルであるリモート・デスクトップ・プロトコル(RDP)のリモート・アクセス認証情報を利用してアクセスすることができます。しかし、悪質なアクターはRDPセッションをエクスプロイトしログイン認証情報を盗み出し、通常の企業の保護機能による検知を回避して、高価値情報の身代金を要求する方法を開発しています。

我々の調査では、ダークネット・プラットフォーム上に多数の情報源があり、認証情報 1 つにつき 2 ドルから 30 ドルで購入できることがわかりました。ダークネット上には、空港のセキュリティへのアクセスを許可するRDPさえあります。[12] この発見は他の研究者によっても裏付けられており、中国や南米のシステムへのアクセスは特に人気があります。Ultimate Anonymity Services (UAS) プラットフォームだけでも、中国の 7,000 件以上、ブラジルの 6,000 件以上の認証情報が販売されていることが判明しています。アメリカのRDPもカリフォルニア州、オハイオ州、オレゴン州、バージニア州を中心に揃っていました。[13]

アクセスに関しては、キーロガーやエクスプロイトよりもRATの方が好まれるという調査結果が出ています。平均すると、キーロガーやエクスプロイトを発見あるいは提供される頻度の約5倍の頻度でRATを発見あるいは提供されました。RATは、犯罪者が離れた場所からネットワークを制御することを可能にし、ハッカーがウェブカメラを起動したり、スクリーンショットを撮ったり、ユーザーの行動を監視したり、クレジットカード番号などの機密情報にアクセスしたりすることを可能にします。

この種の攻撃が再び流行していることは、リストを見れば明らかです。例えば、銀行の認証情報を盗むことができるバンキング型トロイの木馬Ramnitは、2010年に初めて検知され、2018年に銀行に最も広まった脅威となりました。2017年から2019年にかけて、RATを利用した西アフリカの銀行に対する攻撃のウェーブが検知されました。[14]



DNS Messengerのような人気のあるRATは10ドル前後で販売されていますが、デスクトップを遠隔操作できる’Diamond Rat’のような廉価版は2ドルで販売されています。一般的に、システムに特化したツールになればなるほど価格は上昇する傾向にあります。[15]

Macユーザーのデータの多くを監視できるMacSpyのように、Maで動作するバージョンはほとんど検知されないようなので、Macを使用することの多いクリエイティブ業界にとっては特に危険な存在となっています。[16]

図.1：人気のあるRATは10ドル前後で販売されていますが、’Diamond Rat’のような廉価版は2ドルで販売されています。

[12] Zorz （2018年）
[13] Trend Micro （2017年）
[14] Ilascu （2019年）
[15] Migliano （2018年）
[16] Paganini （2017年）

他にも、Androidシステムを利用した新しいRATが、メッセージングサービスTelegramをエクスプロイトし、犯罪者がSMSメッセージを送信したり、通話を録音したり、アプリをインストールしたりすることを可能にしていることが判明しています。[17]

ベンダーは様々なビジネスネットワークへのアクセスを提供しています。医療、銀行、およびリテール/Eコマース分野におけるネットワークへのアクセスは、以下の表3に示されるように、特に広まっているようです。

業種	アクセスを提供しているベンダーの%
医療	24
銀行	18
Eコマース/リテール	16
教育	12
ファイナンス	11
その他	19

表3：ダークネットベンダーがアクセスを提供している業種

1.3.3 標的型攻撃とスパイ活動

標的型攻撃に関しては、ダークネット上のマルウェアは売り手市場となっています。カスタムメイドのマルウェアのリクエストが、既製品のオファーよりもはるかに多いことがわかりました。これは、マルウェア作成の依頼が、実際に提供されるものを約2対1で上回っているだろうという他の示唆を裏付けています。

ほぼすべてのベンダーが、アクセスあるいは被害を与えたいネットワークに応じて「より効果的」に動作するツールを提供してくれました。攻撃のターゲットを絞れば絞るほど価格は高くなります。そして、銀行などの価値の高い企業をターゲットにする攻撃の可能性がある場合には価格はさらに上昇しました。

企業への標的型攻撃の平均額は約4500ドルで、個人への攻撃のコスト（約2000ドル）よりも高くなっていました。例えば、ダークネット上のEmpire Marketのある買い手候補は、PayPalまたはPayPalを利用する個人を対象としたサービスを要求しており、ユーザーアカウントへのアクセスを提供し、お金の送受信をブロックできる場合には最高2,500ドルを提供するとしていました。

発見されたマルウェアの中で最も高価なものの一つは、銀行のATMを標的にした（ATMロジックを攻撃）マルウェアで、約1,500ドル[18]で販売されていました。ATMがお金にアクセスするための最新の方法ではなく、現金には制約があることを考えると、これは少々驚くべきことでした。これについて質問すると、あるベンダーは「古い方法が最も信頼性の高い方法であることもある。そして、検知されるリスクははるかに低い」と述べています。

研究員がFTSE100の企業リストやフォーチュン500の米国企業リストを標的とした依頼をダークネットのハッキングサービスに依頼した場合、約**40%**から肯定的な回答を得ました。特定の企業を標的にした依頼をした場合も、ベンダーからほぼ全てのケースで肯定的な回答を得ており、多くの場合ハッキングを実施するための様々なサービスプランが提示されました。交渉価格は、企業によって異なりますが、150ドル～10,000ドルの間でした。

[17] Vigliarolo （2018年）
[18] 裏付けはInfosec （2018年）参照

標的型攻撃サービスの量は、企業活動に対するスパイ活動の需要が高いことを示唆しています。FBIのデータでは、2015年から2016年の12ヶ月間に、米国企業を対象とした経済スパイの可能性に関連した調査が53%増加していることが強調されています。[19]

比較的オープンなフォーラムでは、スパイに関するデータを入手するのが難しかったので、一歩踏み込んで調査しました。

(i) ハッキングサービスを提供しているベンダーに、直接または標的型のスパイ活動に従事する準備があるかどうかを尋ねました。先の調査結果が示唆しているように、質問したベンダーの約60%が特定のネットワークへのアクセスを提供していると主張しています。

(ii) Telegramメッセージングサービスを利用して、特定の料金でのスパイ活動を明確に要求する通信を行いました。48時間以内に30件の回答がありましたが、法的な理由でそれ以上には進みませんでした。

一般的に、スパイ活動が行われている場合には、2つの形態があることがわかりました。

(i) 単純スパイ：個人が自分の利益のために機密情報を取得しようとする場合。ここでの目的は通常、金銭的な利益です。

(ii) 代理スパイ：スパイ活動の試みが、他の人（通常はクライアント）に代わって行われる場合。第 3 節と第 4 節では、企業自身がどの程度このような活動に関与しているかを検討しますが、国家などの他の依頼人も考慮する必要があります。

図2 ：Empire Marketのサイト会員がAT&Tとベライゾンの情報を集めるためにインサイダーを探している様子

調査中に、アクセスを求めている個人がスパイを企てている例を発見しましたが、その多くはインサイダーを勧誘する方法で行われました。図2に示すように、ある人物は、AT&TまたはVerizonの内部関係者を探し、コンタクトすると、主に会社の契約や給与体系の詳細に興味を示しました。

企業が互いにスパイ行為に従事しているという決定的な証拠を見つけるのははるかに困難であり、ダークネットがどの程度これを促進したかを立証するのはさらに不確実です。驚くことではありませんが、ダークネット上でさえ、企業はこの種の違法な活動に積極的に取り組んでいるという具体的な痕跡を残すことを好みません。

その結果、調査では、営業秘密がダークネットを介して販売されている証拠は見つかったものの、これに関与したのが企業自身であるという直接的な証拠は見つかりませんでした。このシリーズの次回のレポートで詳述する予定ですが、検証は困難なものの、産業スパイの加害者としての国家の証拠も有力なものがあります。例えば、中国による米国の企業秘密の窃盗は、年間 6,000 億ドルに上ると推定されてます。[20] このように大量の脅威が容易に利用できるため、組織はスパイ活動の犠牲にならないように警戒する必要があります。

[19] Kahn （2018年）
[20] US IP Commission （2017年） http://ipcommission.org/

1.3.4 サポートサービス

脅威のレベルは低いですが、それでも懸念されるのは、視聴者に攻撃を仕掛ける方法を教えるチュートリアルが広く公開されていることです。これらのベンダーが攻撃を仕掛けているわけではありませんが、このような情報にすぐにアクセスできるようになることで、これまで以上にスキルアップやサイバー犯罪への関与が容易になり、新世代のサイバー犯罪者を生み出すことにつながります。

例えば、私たちは「ヌーブ」（経験の浅いハッカー）を装い、様々なサービスプロバイダに、完全にカスタマイズされたハッキングシステムのセットアップの助けを求めました。ベンダーのsixandeightは、カーディングを行うための完全なシステムを提供してくれました。

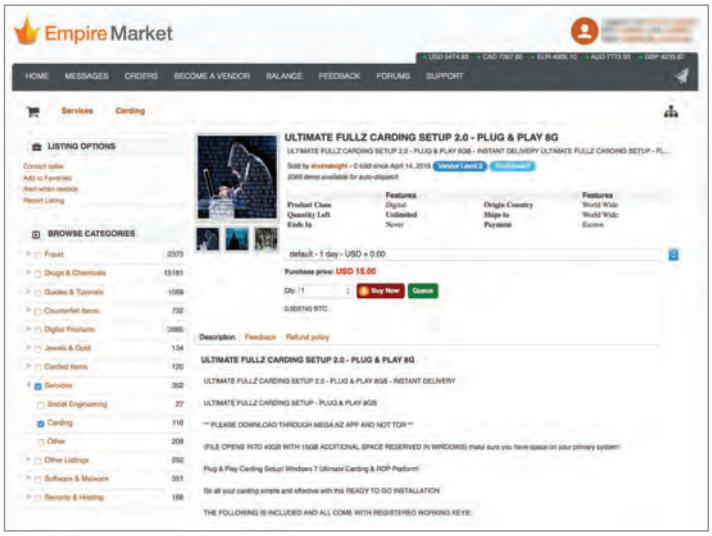


図3 ：Empire Market上のベンダーが我々にオファーしたカード詐欺用のシステム一式

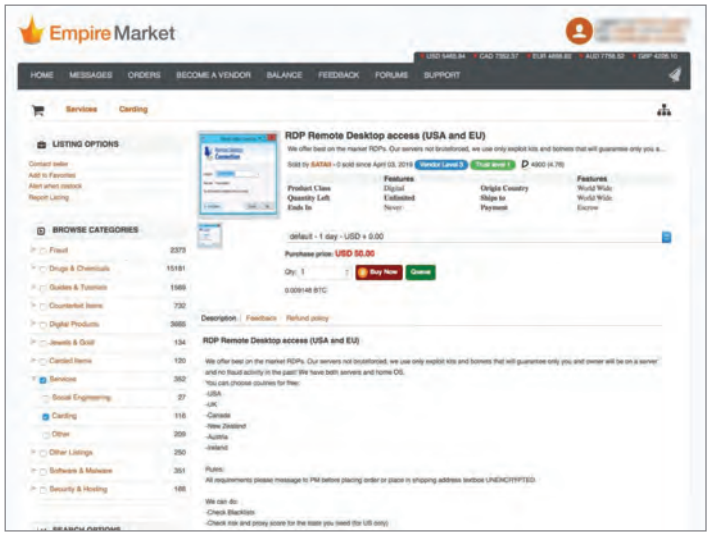


図4 ：あるベンダーは手厚いサポートとクリーンなサーバー付きのリモート・デスクトップ・プロトコルを提供

同様に、ベンダー”SATAII”は、広範なリモート・デスクトップ・プロトコルを提供していましたが、充実したサポートと、過ヰに不正行為の記録がない希望する国のクリーンなサーバーの利用が付属していました。

また、パーソナライゼーションと攻撃を可能にするための顧客サービスに力を入れていることも明らかになっています。特に、「エンドツーエンド」のハッカーサービスがかなりの数に上っていることがわかりました。これは、範囲がより限定されているバンキングスタイルのトロイの木馬の配布に取って代わり始めています。

同じようなトレンドは、クライアントが独自に作成したマルウェアを登録し、それを配布することを可能にする、トラフィック分散システム（TDS）21 の出現にも見られます。いくつかのベンダーは、これらのシステムは、我々が指名したビジネスに対するカスタマイズされたマルウェア攻撃に特に適していると我々に保証してくれました。

1.4 – 金銭的な侵害を可能にするために販売されているツールやサービス

金銭的価値や富を引き出すために使用できるツールやサービスの販売は、サイバー犯罪経済の根幹を成すものであり、その収益の約 50%は詐欺などの活動から得られています。[22] 主要な富の生成者である企業は、サイバー犯罪者にネットワークへの直接アクセスが提供され、独自の攻撃を設計・編成できるようなツールが販売されているため、明確な標的となっています。

[21] BlackTDS の使用例については、Proofpoint (2018)を参照ください。
[22] サイバー犯罪の収益のすべての内訳については、Web of Profit (I)を参照ください。

これらは、各カテゴリー内の代表的なアイテム、各カテゴリーのアイテム占有率の平均値[23]、アイテムの平均価格、およびカテゴリー全体の3Dエンタープライズ脅威評価[24]とともに、下の表に示されています。また、この表には、第3節で後述する金銭的攻撃ツールとサービスのデータも含まれています。

カテゴリー	アイテム	平均 %	平均 価格$	3D脅威 スコア	3D脅威 レベル
金銭的な攻撃					
認証情報	クレジットカード情報	38	2+	28	高
フィッシング・ツール	フィッシング・ツールとサービス	27	5+	28	高
返金などの詐欺	偽造レシート	14	6+	19	中
その他	-	21	-		評価無し

表4：ダークネット上の金銭的攻撃ツール

1.4.1 カードの認証情報

パスワード、CVV番号、有効期限などのクレジットカードやデビットカードのデジタル認証情報は、ダークネット市場で流通している金融関連の商品の中で最も身近で一般的なタイプで、全リストの約38%を占めています。これらはサイバー犯罪の定番商品ですが、ダークネットのビジネスモデルがより大規模データ化するにつれて、販売量は増加しているように見えます。他の調査によると、10億件以上のクレジットカードのデータベースがダークネット上で販売されていることが判明しており[25]、盗難にあったクレジットカードデータの約40%がダークネット上のプラットフォームにあると推定されています。[26]

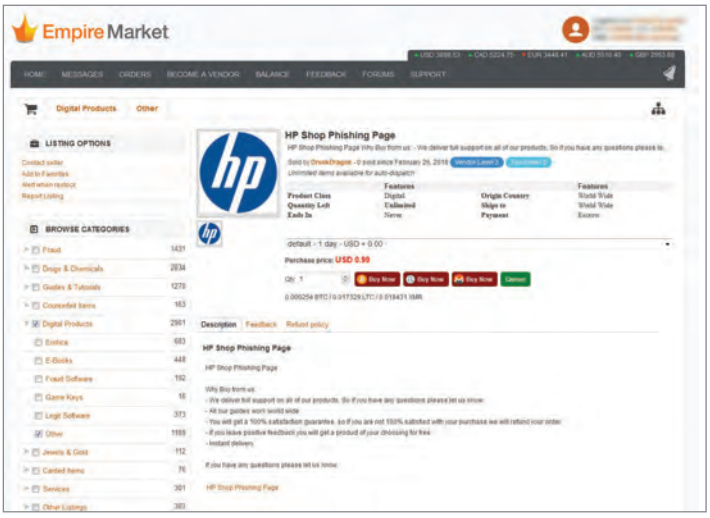


図5：あるベンダーはHPのフィッシング・ページを0.99米ドルでフルサポートと返金保証付きで提供

1.4.2 フィッシング・ツール

ダークネットで販売されているフィッシング・ツールの存在はよく知られています。ダークネット市場（金銭的攻撃カテゴリ）の**27%**がフィッシング・ツールに関連しており、その大部分が企業に対して簡単に利用できる可能性があることがわかりました。

中には、人気ブランドを装った巧妙にデザインされたなりすましページを使って、被害者をおびき寄せて個人情報を提供させ、間接的に悪用するものもありました。例えば、DrunkDragonというベンダーは、HPやAmazonのページをわずか0.99ドルで提供していました。(図5と6)

[23] 各ドメインを100%として扱い、ダークネット・プラットフォームにある他のアイテムを除外して算出。医薬品はどのカテゴリーにも含まれていませんが、これは販売量が多く、各カテゴリー内での微妙な変化が不明瞭になる可能性があるためです。
[24] 3D脅威アセスメントのスコアは、本レポートの方法論のセクションに記載されています。
[25] Casal（2017年）
[26] Equifax（2018年）

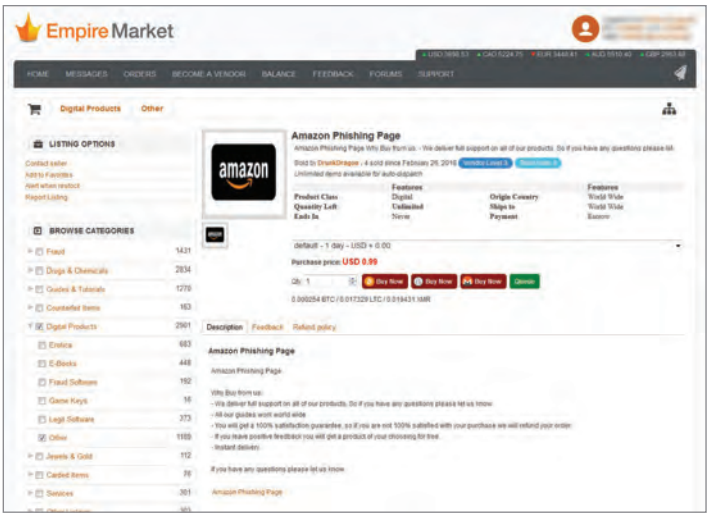


図6 ：あるベンダーはAmazonのフィッシング・ページを0.99ドルで提供。商品説明によると、このようなページはすでに4つ販売。

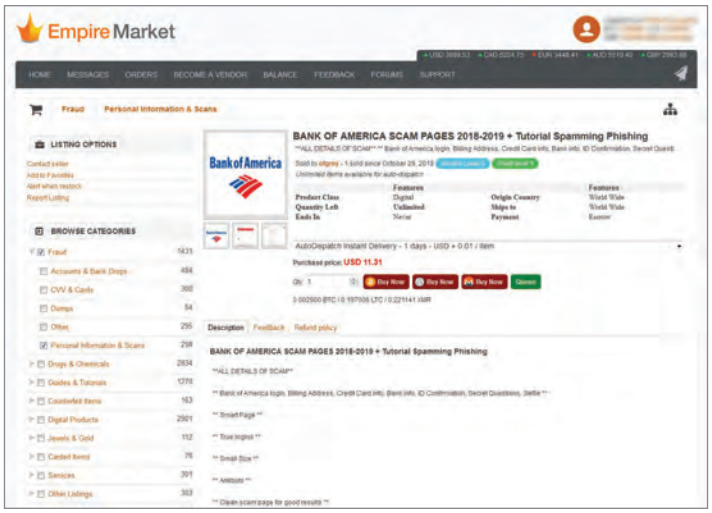


図7： Bank of Americaのなりすましサイトはチュートリアルサポート付きで11ドルで提供

また、ベンダーOfgreyは、Bank of Americaのなりすましウェブサイトのページとチュートリアルサポートを11ドルで提供していました（図7）。

AppleやNetflixのような企業や、TescoやWalmartのような人気小売店を装ったページなど、他にも多くの例がありました。また、MinecraftやLeague of Legendsのようなゲームサイトのなりすましページも、フィッシングリンクをクリックするように被害者を誘導するためによく使われています。このようなページはわずか数ドルで売られていますが、Appleのような需要の高いページやステータスの高いページは通常、それ以上の価格で販売されています。

より進んだツールもあり、最近では40ドル以上で販売されているフルサービスのフィッシング・キットがトレンドとなっています。これらの高度なフィッシング・キットは、データを収集するためのなりすましサイトを自分で構築するためのツールを顧客に提供しています。

他の例としては、南米のユーザーをターゲットにした[A]pacheフィッシング・キットがあり、なりすましサイトに類似したドメイン名（例：Walmart- shopping.com）を作成する機能を提供しています。このキットには他にも、郵便番号の自動検索機能など、被害者に本物だと思わせるための細かな機能が多数含まれています。[27]

企業を標的にしたフィッシング攻撃は、非常に被害が大きくなる可能性があります。例えば、サイバー犯罪集団Carbanakが2017年に行ったフィッシングメールキャンペーンは、Chipotle、Arby's、Chili'sといった米国のレストランチェーンを狙ったものでした。1,500万件以上のクレジットカード情報が盗まれ、数百万ドルの被害が発生しました。この攻撃は、レストランの従業員を誘導して、ケータリングの注文やビジネスに関連するその他の事項が記載されていると思われるメールのリンクをクリックさせることで行われました。[28]

1.4.3返金などの詐欺

私たちは、不正な返金要求を通じて組織にお金を渡すように仕向ける、ダークネット市場が繁栄している証拠を発見しました。Visaは、チャージバックの80%以上が詐欺に関連したものであることを示唆しており、企業は2020年までにこの方法で約250億ドルの損失を被ることになります。[29] 盗まれたカード情報へのアクセスは、チャージバックや「フレンドリー」詐欺の重要な要因となる可能性があります。

[27] Wiat （2018年）
[28] Ng （2018年）
[29] Chargebacks （2019年）

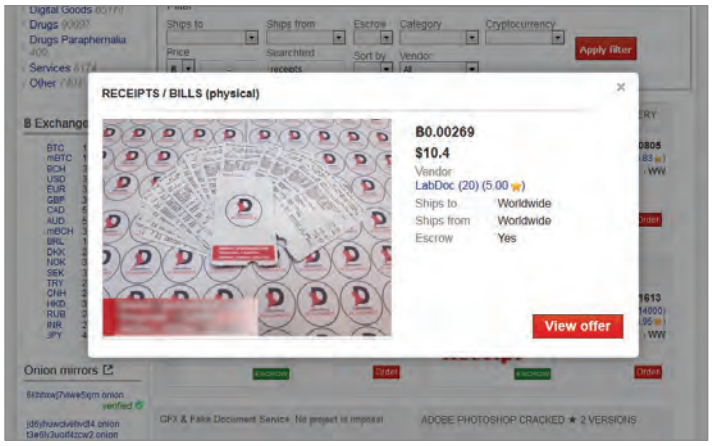


図8 ：あるベンダーはあらゆる種類の領収書の物理的コピーの提供をオファー

これは、犯罪者がダークネット・プラットフォームを介して入手したクレジットカードでオンライン購入を行い、その後、自分のクレジットカードへの請求に異議を唱えるというものです。その後、銀行は返金を余儀なくされ、顧客は不正に入手した購入品を保持し続けます。

返金を得るために偽の領収書やその他の書類を提供することも人気のある手法の一つです。例えば、私たちはLabDocと呼ばれる業者に連絡を取りましたが、彼らはどんな種類の業務用領収書や請求書でも物理的なコピーを作成できると自慢していました。(図8)

同様にDenというロシアの業者が、返金を得るためのAmazonやAppleの請求書を提供していたことが判明しました。(図 9、10)

図9： ロシアのベンダーが返金を得るためのAmazonとAppleの請求書を提供

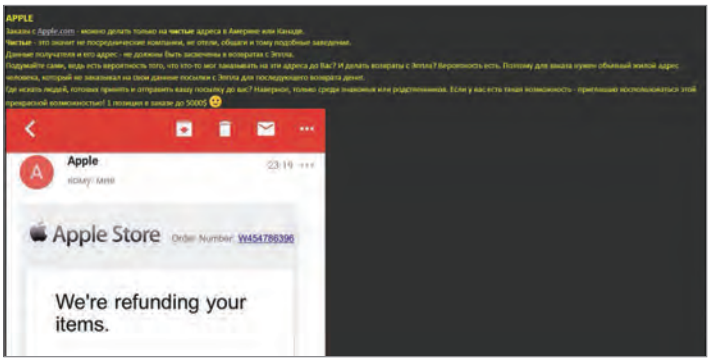


図.10 ：ロシアのベンダーがAppleからの高頻度返品顧客フラグ回避のための実在人物の「クリーンな」自宅住所を潜在顧客に宣伝

1.5 – データを侵害するために販売されているツールやサービス

多くの意味で、データのダークネット取引は、クライムウェアの取引と同じくらい企業にとって脅威となっています。我々の調査によると、ダークネット・プラットフォームで取引されているアイテムの中で、データは薬物に次いで2番目に普及しており、現在ダークネットで利用できるデータの種類の多さには驚かされます。

私たちの調査と他の推測を組み合わせると、ダークネット活動の25 ~ 33%が企業データの売買に関連していることが示唆されます。[30] 被害には、以下のような強力な組み合わせが含まれている可能性があります。その被害は、評価の低下、混乱、詐取の組み合わせとなります。さらに、データの価値の低下、顧客の信頼の喪失、スタッフの士気の低下、企業に対するネガティブなイメージの上昇、データ侵害対策のためのセキュリティへの追加支出などを含みます。

しかしながら、データ漏洩の責任の特定は、不確実の高い問題です。 確かに、個々の実行犯がセンシティブな情報を伝えようとしている証拠はあります。データ漏洩の少なくとも半分は、企業の内部関係者が関与していると言われており[31]、その大半は、経営陣やIT部門ではなく、下っ端の従業員が関与していると考えられています。

[30] Filecloud （2018年）
[31] Allen （2018年）
[32] Preston （2019年）

さらに、競争相手に転職した高位の元従業員にも大きなリスクが潜んでいます。機密情報の取得は非常に簡単な場合もあり、転職した従業員の最大 13%が、元の認証情報を使って以前の雇用主のネットワークにアクセスできると考えられています。[32]

その他のリスクとしては、自分のデバイスを職場に持ち込むことができる従業員（BYOD）や、単純に退社前にデータやファイルをコピーする従業員が挙げられます。その結果、多くの企業では、機密情報を扱う従業員に対し、競合他社との雇用関係を結ばないことや、企業の情報を利用して独自のビジネスを開始しないことを義務付ける「非競合」条項の締結を義務づけています。

ダークネット・プラットフォームでオープンに取引されている企業データは、大きく分けて4つのカテゴリーに分類されています。これらは、各カテゴリー内の代表的なアイテム、各カテゴリーのアイテム占有率の平均値、アイテムの平均価格、およびカテゴリー全体の3Dエンタープライズ脅威評価[33]とともに、下の表に示されています。これは、ダークネット・プラットフォーム上の他のカテゴリーにリストされているアイテムを除いたものです。

カテゴリー	アイテム	平均 %	平均 価格 $	3D脅威 スコア	3D脅威 レベル
データの窃盗					
顧客データ	口座の詳細情報	28	10	25	高
	銀行/他のログイン	21	5		
	対応履歴	4	20		
業務データ	ビジネスEメール	15	10-50	17	中
	社内コミュニケーション	5	35		
財務データ	請求書	14	5-10	23	高
	年次決算	6	60+		
営業秘密と知的財産	すべての種類	不明	不明	16	中
その他		7			評価無し

表5 ：ダークネットで取引されている企業データ

1.5.1 顧客データ

顧客の詳細情報がダークネット上で発見されると、企業にとって大きな頭痛の種となり、信頼の毀損、風評被害、取引の中断、収益の損失、修復にかかる時間と費用、さらには潜在的には株価の下落や投資家の信頼を失うことになります。

サイバー犯罪者にとって、金融データは明らかに優先度が高く、2017年 ~ 2018年に銀行から顧客データ（口座のログイン情報やクレジットカード情報など）の取引が135%増加したと報告[34]されていることからも、その魅力が継続していることがわかります。

[33] 3D 脅威アセスメントのスコアは、本レポートの方法論のセクションに記載されています。
[34] IntSights （2018年）

フィッシングやアカウントの乗っ取りは、サイバー犯罪者が盗んだデータを利用する方法のほんの一部に過ぎません。漏洩した顧客データはもっと一般的な用途にも使われています。例えば、ある闇ネット業者との会話では、彼が欲しがっているものがわかりました。

> *「...顧客データ - どんな種類のデータでも、我々が必要としているものを情報豊富なデータベースにまとめて提供してくれます。誰かがクレジットカードの利用者であることがわかれば、その人が持ち家なのか賃貸なのか、結婚してしていれば、子供がいるかどうか、何人いるかどうかなどがわかります。仕事や収入、大学進学先まで分かります。」*

ランサムウェアやオンライン上の脅威に特化した業者はこんなことを知っていると言っていました。

> *「政治的なことや、金融投資、どこに旅行従っているかということさえ、すべてが私にとって非常に有益なものです。」*

調査の結果、ダークネット上でその顧客データが取引されている様々な企業を発見しました。その中には銀行や金融機関のデータベースがあり、例えばカタール国立銀行のこのデータベースには顧客のパスワードやPIN番号が含まれていました。

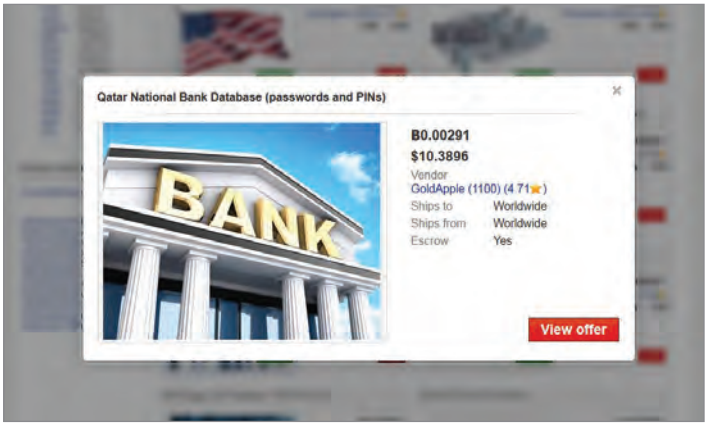


図11 ：ダークネットで販売されているカタール国立銀行のデータベース（顧客のパスワードと暗証番号が記載）

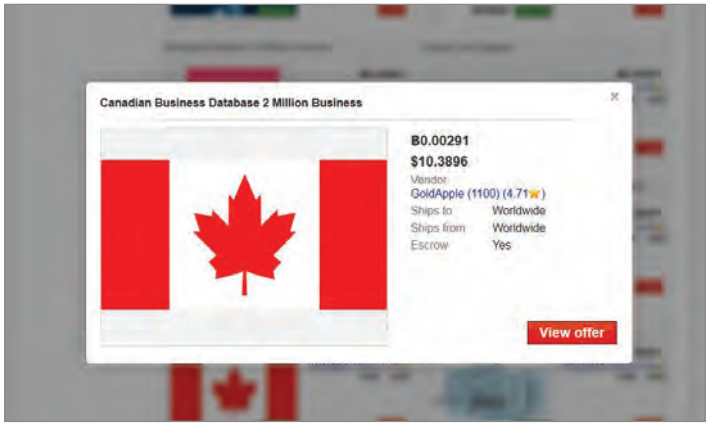


図12 ：200万社以上のカナダのビジネスのデータベースをわずか10ドルで提供するダークネット上のベンダー

最も衝撃的だったのは、国全体のためのデータベースを発見したことです。その一例では、200万社以上のカナダの企業のデータが含まれており、たった10ドルで売られていました。

1.5.2 業務データ

ダークネット上で販売されている顧客データベースが発見されることは、企業にとって恥ずかしいことですが（コストがかかることは言うまでもありません）、より機密性の高い業務データの取引はさらに問題となります。当社の研究者が発見した典型的な商品には、企業の電子メール、請求書などの会計・財務情報、さらには会議の議事録などが含まれていました。ダークネットで取引されているデータのうち**約15%**は、企業の方針や戦略に関連した内容、支払い、従業員の雇用、解雇、辞職、プロジェクト費用などを含む企業の電子メール・チェーンに関連したものでした。この種のデータは、メディアへの情報漏洩の脅しから、企業幹部への脅迫まで、お金になる選択肢を提供します。

FBIのデータによると、2016年 ~ 2018年の間に世界のビジネスメール詐欺が136%増加し、多くは資金移動を要求する侵害されたメールによって、関係する企業に120億ドル以上の損失をもたらしています。[35] また、特定の企業とその企業の買掛金部門を標的とした、より巧妙な詐欺に利用されることもあります。この調査では、ダークネット上のあらゆる場所で、企業の電子メールが漏洩しているという実質的な証拠が発見されました。我々の調査員は、あるオンライン小売業者からOutlookの電子メールのサンプル一式を提供されました。（セット全体の購入を促すために）示されたサンプルメールのいくつかには、企業の年次報告書、解雇や雇用の方針、チームビルディングのイベント、さらには（明らかに脅迫の可能性がある）職場での秘密の恋愛に関するコミュニケーションなど、さまざまな機密情報が含まれていました。

1.5.3 財務データと盗まれた請求書

年次報告書に記載される背景情報のような企業の財務データは、ダークネット上で高価で売られています。私たちの研究者は、いくつかの大手企業のものを提示されましたが、これらは高価で、私たちがフォローアップしようとしたときには、ベンダーは消えてしまいました。

企業の請求書を購入することは、ダークネットで簡単にできますが、私たちが見たものは本物のようで、中には折り目がつき、擦り切れているものもありました。私たちがこれらを何に使用できるかを尋ねたところ、ベンダーはフィッシング詐欺に使用する方法を説明しました。

> *「あなたは、好きな会社から何かを購入したことを示す私の偽の請求書を会社にメールすることができます。購入を承認しない場合は、0.184 XMR ($10) の追加料金で、そのリンクをクリックするように会社に伝えるメールを提供することができます。すぐに、あなたすべての詳細を取得することができます。」*

ここでも、様々な企業が取引されていました。例えば、Goldappleというベンダーは、T-Mobileのインボイスを1枚5ドルで提供していました。

同じベンダーがCathay Pacificの請求書を同額程度で売っていました。

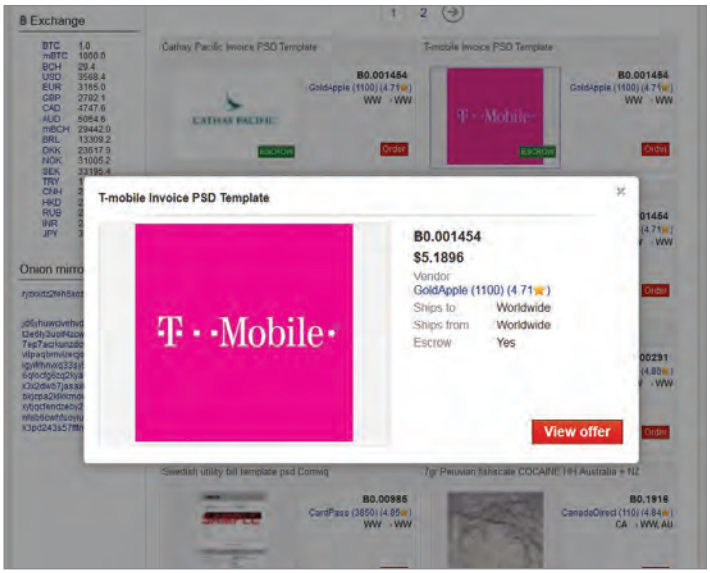


図13 ：T-Mobileの請求書の偽造品が1枚5ドル

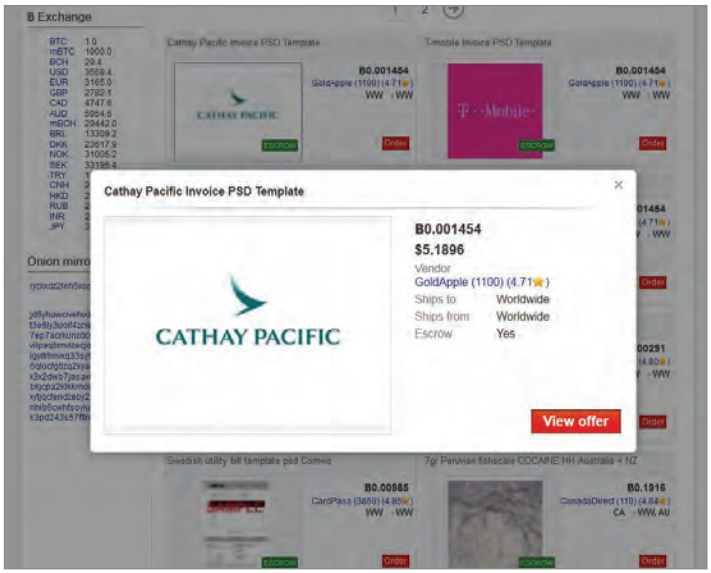


図14 ：ダークネットのCathay Pacific偽造請求書

[35] FBI （2018年）

1.5.4 営業機密と知的財産

ダークネット上でのデータ取引は、営業秘密や知的財産の取得と売却を伴う最も深刻な取引である可能性があります。この取引の多くは非常に秘密裏に行われていますが、私たちが知っているのは、このような取引が存在し、ダークネットがそのための安全な避難所になりつつあるということです。Enigmaダークネットフォーラム（現在は廃止）には、標的となっている企業のインサイダーとして活動するために募集されたメンバーの名前がありました。また、恐喝のために利用できる可能性のある従業員についての情報も求められていました。

私たちの研究者は、この種のまだ稼働しているプラットフォームを多数探しましたが、この取引は今ではさらに隠密化しているか、あるいは「インビジブル・ネット」に移行しているようです（その詳細については、このレポートの後の方でご紹介します）。しかし、私たちが話を聞いたフォーラムのメンバーの一人は、特定のクライアントに代わって知的財産や営業秘密を取得することで、大金を稼いでいることを示唆していました。試しに、私たちは彼に大手企業3社の名前を提供し、どのようなスパイサービスを手配できるかを尋ねました。彼は1,000ドル～1万5,000ドルの間で、CEOやその他のエグゼクティブ・コミュニケーションへのアクセスや、「彼らのサーバーから欲しいものを何でも手に入れる」ことを提案しました。これらの主張を検証する方法はありませんでしたが（スパイ活動をしない限り）、彼は、一般には公開されていない会社のある情報を提供し、彼が本物である可能性を示しました。

2 – 企業に関連する伝統的犯罪のダークネット化

ダークネット上で利用可能なツールが示す情報や金融のセキュリティに対する明白な脅威に加えて、以下のような明白ではないサービスも発見しました。表向きは無害ですが、企業の成功に向けて長期的に重要な問題を提起する可能性があります。

2.1 – ダークネットでのインサイダー取引

ダークネットの隠されたプラットフォーム、招待制のフォーラム、プライベートメッセージシステムは、本質的に匿名性の高い空間であるため、株取引に関する秘密を共有したり、ライバルの投資家よりも優位に立とうとするのに適しているように思われます。私たちは、この種の情報を提供すると主張する少なくとも2人の人物と接触しました。

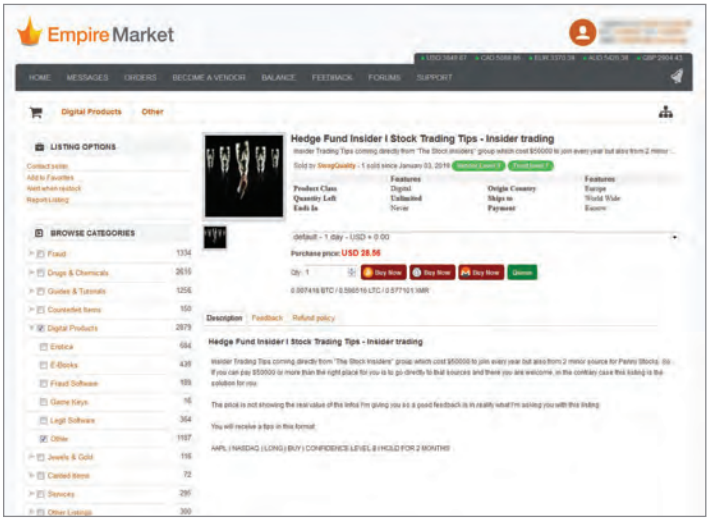


図15 ：Empire Marketプラットフォーム上のベンダーが提供しているヘッジファンドのインサイダー情報

例えば、Swag Qualityというベンダーは、ヘッジファンドや株式市場の取引に関するインサイダー情報を提供し、他よりもはるかに安く購入できると主張していました。しかしながら、 情報の一部は 疑わしいStock Marketのインサイダー・プラットフォームから 取得されたように見えました。

私たちが接触した他のベンダーは、Tescoのような小売業者に加え、いくつかの銀行や投資会社など、さまざまな企業のインサイダー情報を持っていると主張しました。このように、ダークネット上でインサイダー取引が行われているのではないかという疑念は、正当なものであると思われますが、それはもっと目に見えない場所、特にTelegramのような暗号化されたメッセージングツールに限られていると思われます。

2.2 – 採用と不正行為

偽の認証情報や身分証明書は、特に好調な市場を提供しています。本調査では、偽の雇用証明書やほとんどすべての主要な高等教育機関の偽造学位証明書を含む様々な偽の書類が販売されていることがわかりました。多くのベンダーは、幹部レベルから現場に至るまで、様々な応募者のトップポストを確保するのに役立つと主張し、大学や以前の雇用者のデータベースをハッキングして記録を改ざんしたり、偽の推薦状を作成したりすることさえ提供していました。以下の例を参照ください。

図16 ：購入者はダークネットでほとんどの大学の偽の学位を見つけることができる

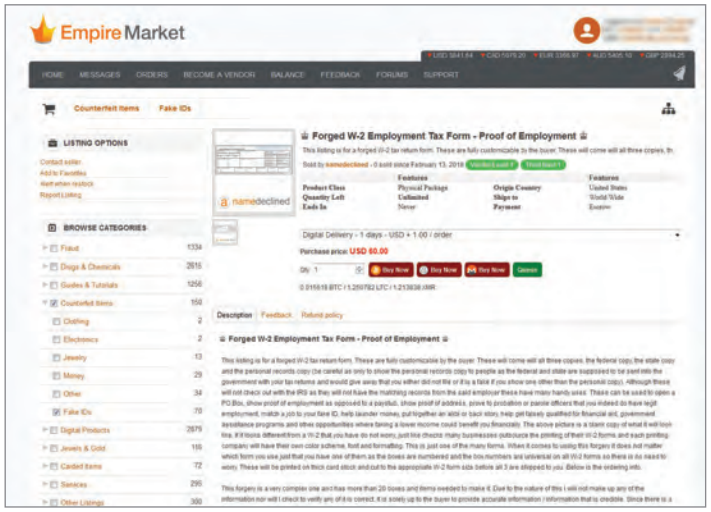


図17 : ダークネットで公然と販売されている偽造W-2申告書

図18 ：Quick Fix尿検査キットは、必要な薬物検査に合格するために設計されています。多くの場合、返金保証が付いています。

確立された安全基準を回避するサービス（薬物検査やアルコール検査など）も広く利用できるようになっていました。航空会社のパイロット、列車の運転手、バスの運転手、重機の運転手など、多くの仕事では、従業員は定期的な薬物検査を受ける必要があります。ダークネットは、これらの安全検査を回避したり、なりすましたりするための様々なツールを提供しています。我々は職場の尿検査での検知を回避するためのツールを見つけましたが、その多くは返金保証などの宣伝がついていました。

3 – 企業とグレーネット：ダークネットの準法的利用

犯罪者がソーシャルメディアのような合法的なプラットフォームを利用する方法を学んだように、企業は知らず知らずのうちに、常に法律の厳密な範囲内にあるとは限らないダークネットの利用に引き込まれることがあります。このような状況がいつ、どのように発生するかを特定することは容易ではありません。あまりにも公然と違法または半違法な活動に従事することは、企業のブランドを損なうリスクがあり、法の執行機関の注意を引く可能性もあります。しかし、時には企業が法の境界線上で活動していることを示唆する十分な指標があります。

3.1 – 競合情報分析か企業スパイか？

ライバルがどのように経営しているかを企業がよりよく理解しようとする「競合情報分析」活動は、ダークネットに簡単に移すことができます。例えば、市場でライバルを弱体化させるセキュリティの弱点を取得することに使える情報があるかもしれません。またはブランドの権威を損なうのに使用することができる偽造品の証拠があるかもしれません。 あるいはフォーラムは消費者の意見をテストすること、もしくは否定的な噂を広めるためにさえ使用することができるかもしれません。

中規模企業のビジネスソフトウェア部門代表者を装い、20ベンダーに連絡を取り、標的型攻撃によって以下の「当社にとって関心のある項目」を提供してもらえるかどうかを尋ねました。ほとんどのベンダーはフォーラムでの議論を拒否し、私たちが彼らにプライベート・メッセージを送るか、暗号化されたメッセージングサービスに移行してからでないと詳細を教えてくれませんでした。彼らの回答の内訳は以下の通りです。

要求した情報	肯定的な回答をしたベンダーの数	「さらに引き合いすすめる」と回答したベンダーの数	返信がなかった数
商品の試用	10	2	8
従業員リスト	14	0	6
年次決算	4	11	5
役員給与	7	5	8
CEO/役員の出張プラン	3	3	14

表6：企業情報の提供を求めたベンダーの対応

私たちがサービスの頭金を提供しなかったため、すぐに不審に思い、攻撃的にさえなったベンダーもありました。ほとんどの業者はそれ以上の連絡を拒否し、（多少の言い換えになりますが）「自分の身がかわいいなら、このスレッドから離れろ」と言ってきたベンダーもありました。

3.2 – ブラックリストの共有

ブラックリストの共有は、不正なウェブサイト、新しいマルウェアの脅威、問題のある顧客/従業員/請負業者などを含むかどうかに関わらず、組織にとっては明らかに魅力的なものとなっています。最近行われたGlobal Fraudの調査[36]によると、調査対象となった企業の96%が顧客のブラックリストを保管していることが示唆されています。しかし、動機は不正行為だけではありません。E コマースの小売業者は、問題を起こすと思われる顧客をブラックリストに登録することがよくあります。例えば、最近Amazon で何百もの商品を購入した顧客が、購入した商品を何度も返品したためにブラックリストに登録されました。この種のリストを我々の調査員に提供できると主張するダークネットベンダーも数多くありました。それには2万人までの名前と詳細が50ドルという低価格にもかかわらず、リストには個人の名前、クレジットカードの詳細、電子メールや住所が含まれていました。問題を起こすと思われる個人の情報を企業が共有することは、新しいスタッフを採用する際の潜在的な被害を避けるためにも魅力的です。しかし、多くの場合、これは違法です。

[36] MRC （2017年）

4 – 企業によるダークネットの合法的な商業化

ダークネットは単なる犯罪的不公正の巣窟ではありません。企業がダークネットを活用する新しいビジネスモデルが登場しています。ダークネットの合法的な商業利用は、プライバシーに関する懸念の高まりに直面して成長しています。例えば、Facebookには毎月100万人以上が利用しているダークネットサイトがあることがわかっています。[37] また、他にも多くの合法的な利用方法があり、ますます普及しています。

4.1 – サイバーセキュリティ

ネットワークと顧客のセキュリティを強化するためにダークネットを使用することができることは企業にとって明らかな利点です。潜在的な脆弱性や新たな脅威についてサイバーセキュリティチームに警告することができるダークネットフォーラムには、豊富な情報があります。企業に対して使用されている新しいハッキングに関する高度な情報や、ボットネットや侵害されたサーバーなどのツールに関する知識は、企業が自社のサイバーセキュリティの手法を開発する際のコストを大幅に削減することができます。また、ダークネットの活動を監視することは、例えば、フィッシング攻撃から身を守るためや顧客データが漏洩しダークネット上で販売されている場合にも非常に役立ちます。

4.2 – セキュアな通信

情報源との通信に安全な通信を利用できることは報道機関にとって魅力的です。その結果、Propublica（https://www.propublica.org/）のような調査報道機関は、現在、独自のダークネットサイトを持っています。また、警察や政府機関と共有する活動を監視するためにダークネットを使用する国連のような他のタイプの機関によるダークネットの利用も増加しています。

4.3 – ビジネスインテリジェンス

政府が主導したTorネットワークの本来の機能の一つは、安全な通信を確保することでした。このように、ダークネットは、インテリジェンスの収集と共有に理想的なメディアであることは間違いありません。企業もこのようにダークネットを利用することに競争上の優位性を見出し始めたのは、驚くに値しません。ダークネット上には膨大な種類の、いわゆる「ダークデータ」と呼ばれるデータがあり、企業は消費者の嗜好の理解を深めるなど、顧客の洞察を深めるために利用することができます。ダークネットのデータは、業務、マーケティング、新製品の洞察力を得るためにマイニングすることも可能です。企業はこのような情報を自分たちで収集することができますが、ダークネット情報を企業に提供する新興の産業が増えています。

4.4 – 信用調査

Experian [38] ようないくつかの信用格付け会社は、すでに顧客の詳細（SSN、電話番号、ID情報）がダーク・ウェブ上にあるかどうかをチェックするサービスを提供しています。これは、貸し手や他の信用機関が融資を査定する際に、申請者の信用履歴を調べる際にダークネットからの洞察力を得ることで、追加の安全措置を構築する可能性があることを示唆しています。

4.5 – リクルート

従来の人材紹介会社では手の届く可能性の無いコミュニティにリーチする新しい方法を提供しているため、一部の企業がリクルートのためのツールとしてダークネットを利用しているという証拠もあります。例えば、Cicada 3301 [39]と名乗る匿名の組織が行ったキャンペーンでは、複雑なパズルを次々と投稿し、最終的に候補者をダークネットに誘導しました。この組織の正体は謎のままですが、ここには想像力に富んだ採用のための明確な前例があります。ダークネットが提供する求職者に関する高度な情報と合わせて考えると、人事や求人は、ダークネットの利用が進むにつれて進化する可能性のある数多くの業務の一つであることは明らかだと思われます。

---

[37] Wong （2016年）
[38] Experian Information Services: https://www.experian.com/consumer-products/free-dark-web-email-scan.html
[39] Nadel （2018年）

4.6 – ダークネットに関わることの潜在的なリスク

潜在的なメリットがあるにもかかわらず、企業はダークネットに関わるリスクに注意する必要があります。1つ目は、マルウェアにさらされるリスクの増大です。第二に、クリアネットに適応したビジネスモデルの混乱の可能性です。多くの企業にとって、それが Facebook、Twitter、Googleのようなプラットフォーム資本主義の巨人であろうと、小規模で機敏なビジネスであろうと、規制要件の増加によりコストが上昇し、イノベーションを起こす能力が低下する可能性があります。さらに悪いことに、データ収集とその商業利用に大きく依存している伝統的な収益生成モデルは、匿名の商取引がますます一般的になると、明らかに危険にさらされることになります。

5 – クロージング

企業を脅かすダークネット市場が繁栄していることは明らかであり、この無法状態を取り締まるという課題を解決することは決して簡単なことではありません。私たちは、サービスがすぐに利用できることに驚き、これまで以上に隠密に営業が行われている傾向に懸念を抱きました。今後もさらなる調査が必要ですが、法執行機関と企業の双方に対して、リスク管理に役立ついくつかの重要な提言を行うことができました。これにより、将来的にこのような行為をやめさせ、企業を守ることができると期待しています。

5.1 – 法執行機関への提言

法執行機関の観点からは、ダークネットからの脅威を特定して無力化するために、企業とより密接に協力する必要があることは明らかです。ダークネットから収集した情報を企業と共有する準備を強化することで、特定の脅威、特に特定のネットワークに対する標的型攻撃や、リモート・アクセス認証情報を利用したコントロールの試みに対する脆弱性を軽減することができます。

専門のダークネット・インテリジェンス・ユニットを設置することで、法執行機関のサイバー犯罪活動を阻止する能力が強化されます。サイバー犯罪活動は、クリアネットとダークネットの両方で活動するようになっており、一方が他方を強化することも少なくないからです。これらの交流を追跡することは、サイバー犯罪防止の任務を強化するのに役立つでしょう。また、上述のような「アンビジブル・ネット」の台頭にも注意を払う必要があり、ダークネットがさらに深みにはまってしまわないようにする必要があります。これは重大なリスクであり、さらなる議論と研究が必要です。

5.2 – 企業への提言

企業にとっては、ダークネットを管理するためのサイバーセキュリティ能力を構築するために、ダークネットがもたらす脅威に対する認識を高める必要があります。特に、サイバー犯罪者が企業ネットワークにリモートでアクセスして制御することを可能にする、ダークネット上でホストされているRATなどのマルウェアには、より注意を払う必要があります。また、ダークネット上のRDPの流通は、サイバー犯罪者がビジネスネットワークを支配することを可能にしており、より効果的に監視する必要があります。

企業は、「インサイダーの脅威」に関する知識と理解を拡大し、インサイダーが企業データを共有したり、侵害を支援したりする際にダークネットが果たす役割にまで拡大する必要があります。職場での従業員によるプライベートまたは暗号化されたメッセージングシステムの使用は、ダークネットから制御される DDoS やキーロガーなどの脅威に対するバックドアアクセスを制限するために、より慎重に規制される必要があります。これと RAT の普及により、組織はセキュリティ境界をアプリケーションレベルまで下げ、顧客データ、業務データ、財務データの周りに壁を構築しなければならないことが示唆されています。これにより、たとえRATに感染したエンドポイントかのアクセスであったとしても、これらのデータへの接続を安全にすることができます。

ユーザーをダークネットにリダイレクトするブラウザ検索について管理者やスタッフを教育するためのトレーニングの強化が必要であり、職場でのTorブラウザの使用については、より慎重に監視する必要があります。また、ユーザーの保護も強化する必要があります。

脅威を隔離する仮想化技術は、マルウェアを無害化することで、ここでも役立ちます。従業員はもはや最後の防衛線となる必要はなく、マルウェア感染の心配なく、電子メールの添付ファイルを開いたり、ウェブサイトをクリックしたりすることができます。

また、機密性の高い業務上の詳細、特に企業の電子メール・チェーンがダークネット上で盗まれたり販売されたりするのを防ぐためにも、より大きな注意が必要です。一般的に、ビジネスメールの内容はより慎重に規制されるべきであり、パスワードや財務情報などの機密性の高い内容を含めることについては、より強固なポリシーを策定する必要があります。

また、ダークネットで簡単に入手できる偽造資格を含む採用関連の不正行為の増加を、より厳密に監視する必要があります。企業が警戒すべき代表的なものには、偽の大学卒業証書、医師の手による履歴書、偽造パスポートなどがあります。

しかし、ダークネットがもたらす脅威は、ダークネットが提供できるビジネスチャンスを制限するものではありません。それには、より広く、より多様な顧客基盤へのアクセス、より革新的なマーケティング、そして匿名性を高めることで顧客の信頼を構築する新しい方法の開発が含まれています。企業は、ダークネットを有利に利用するためのリソースを準備しておく必要があります。

特に、インテリジェンスとサイバーセキュリティを目的としたダークネットの利用強化をするための能力を構築すべきです。これには、企業ネットワークの侵害に関与するマルウェアがダークネットのマーケットプレイスで取引されていないか監視したり、企業や顧客のデータが取引されていないか監視したり、フィッシング目的で企業ブランドが悪用されていないか監視したり、なりすましのウェブページや会社の請求書の販売などによるレピュテーション攻撃がされていないかをチェックすることが含まれます。定期的な監視は、企業のIPや商品の偽造品の自由な取引を防ぐことにも役立ちます。しかし、ダークネットの活動が現在の規制の枠組みや法律に準拠していることを確認するためには、常に専門家のアドバイスを求める必要があります。

方法論

研究の方法

本調査の目的のため、2018年11月から2019年3月までの期間に、15の大手ダークネット・プラットフォームの分析を実施しました。この期間中、これらのプラットフォーム全体で7万件以上のリストが調査され、販売された商品、価格、ベンダーの対応、取引パターンなど、さまざまな側面が精査されました。これらのプラットフォームに併設されている3つのフォーラムに参加し、観察、情報収集、秘密の模擬取引などのデータ収集を行いました。さらに広告への対応の一部、あるいは模擬的な購買の過程で、30社のベンダーと定性的インタビューを実施しました。ダークネットのツールやサービスが企業にもたらす脅威の多次元的な性質をよりよく評価するために、脅威評価ツールも開発されました。

本研究では、3種類のメトリクスを使用した混合型アプローチを利用しました。

(i) 調査したプラットフォーム：

- Dream Market
- Empire Market
- Wall Street Market
- Agora
- darkOde
- Point/T-chka Free Market
- Olympus Market
- Ramp (Russian Anonymous Market Place)
- RuTor
- Silk road 3
- Deep Sea
- Berlusconi Market
- IDC
- Wayaway
- ToyouTeam

(i) Empire Market、Dream Market、The Hubの3つのフォーラムでの秘密裏の観察をディスカッション、質問、模擬取引のよる情報収集で実施。

(ii) 広告への対応の一環として、または模擬購入の過程で、30のベンダーと定性的インタビューを実施。

また、エビデンスベースを強化するために、様々な一次資料や二次資料も参照されました。

方法論
つづき

ダークネット脅威評価ツール開発の方法論

データを分析し、ダークネット活動が企業にもたらす脅威を分析するために、3Dダークネット脅威評価ツールを開発しました。潜在的な脅威の12カテゴリーを定義しました（下表参照）。次に、サイバーセキュリティ、サイバー犯罪、法執行機関、企業経営の分野の専門家6名からなるパネルに、それぞれのカテゴリー毎で、ダークネット商品が企業にもたらす脅威をその知識と経験を使って評価するように依頼しました。「脅威」は、企業への被害が発生する可能性のある3つの重要な指標で定義されています。

破壊 – ダークネットのツールやサービスがビジネスの日常機能を損なうこと。

減価 – ダークネットのツールやサービスがビジネスの市場を侵食すること。例えば、競合他社に優位性を与えたり、ブランドへの信頼を損なったりすることによる。

搾取 – ダークネットのツールやサービスが金銭的損失をもたらすこと。

脅威はそれぞれ1 ~ 10の尺度で評価され、それぞれのカテゴリーの合計は**30**になります。スコアは、以下の脅威レベルに関連付けられます。

20 – 30：高い脅威レベル

10 – 19：中程度の脅威レベル

0 – 9：低い脅威レベル

	カテゴリー	3D 脅威スコア	脅威レベル
ネットワーク侵害			
1	感染 /攻撃ツール	**22**	**高**
2	アクセス	**27**	**高**
3	標的型攻撃とスパイ活動	**26**	**高**
4	サポート・サービス	**18**	**中**
金銭的な攻撃			
5	認証情報	**28**	**高**
6	フィッシング・ツール	**28**	**高**
7	返金などの詐欺	**19**	**中**
データの窃盗			
8	顧客データ	**25**	**高**
9	業務データ	**17**	**中**
10	財務データ	**23**	**高**
11	営業秘密と知的財産	**16**	**中**
その他			
12	新興の脅威	**20**	**高**

表 1：調査した各カテゴリーの 3D 脅威スコア

方法論
つづき

	破壊	減価	搾取	合計
ネットワーク侵害				
感染 /攻撃ツール	10	7	5	**22**
アクセス	10	9	8	**27**
標的型攻撃とスパイ活動	9	8	9	**26**
サポート・サービス	6	5	7	**18**
金銭的な攻撃				
認証情報	8	10	10	**28**
フィッシング・ツール	8	10	10	**28**
返金などの詐欺	5	6	8	**19**
データの窃盗				
顧客データ	8	9	8	**25**
業務データ	6	6	5	**17**
財務データ	7	8	8	**23**
営業秘密と知的財産	5	7	4	**16**
その他				
新興の脅威	7	6	7	**20**

表8：各カテゴリーの3D脅威スコアの内訳

参考文献

Allen, P. (2018) Half of data breaches are the fault of insiders, not hackers, research finds, Computing 01/10/2018

Branwen (2019) Darknet Market Archives (2013-2015), https://www.gwern.net/DNM-archives Brignall, M. (2016) Banned by Amazon for returning faulty goods, The Guardian, 18/03/2016

Casal, J. (2017) 1.4 Billion Clear Text Credentials Discovered in a Single Database, Medium, 09/12/2017

Chargebacks (2019) Chargeback Stats, 08/02/2019

Christin, N. (2017) An EU-focused analysis of drug supply on the AlphaBay marketplace, EMCDDA, 11/2017

Cimpanu, C. (2019) Authorities shut down xDedic marketplace for buying hacked servers, ZDnet, 28/01/2019

Darkweb News (2017) Nuke Malware For Sale on the Dark Web, 10/08/2017

Denton, D. (2017) Annual sales estimation of a darknet market, Denton, 25/05/2017

Equifax (2018) How financial crimes are hidden in the dark web, Knowledge Centre (Identity Protection), 2018

Europol (2019) Double Blow to Dark Net Marketplaces, 2019

Experian (2018), Is your information on the Dark Web?, 2018

FBI (2018) Business E-mail Compromise The 12 Billion Dollar Scam, Public Alert Number I-071218-PSA

FDA (2018) FDA launches global operation to crack down on websites selling illegal, potentially dangerous drugs, US Food and Drugs Administration, Press Release, 23/10/2018

Fearn, N. (2018) BT starts sharing malware data with rival ISPs in ‘world’s first’, The Inquirer, 07/02/2018

Filecloud (2018) The Biggest Threats from the Dark Web That Keep Businesses on Their Toes, Security 07/09/2018

Hazlehurst, B. (2016) Meet New Zealand’s 19-Year-Old Jordan Belfort Getting Rich Racketeering on the Dark Web, Vice, 13/10/2016

Hoyme, C. (2018) The Dark Web and its Impact on Small Business, Jackson Lewis Workplace Privacy, Data Management & Security Report, 21/02/2016

Ilascu, I (2019) Banks in West Africa Hit with Off-The-Shelf Malware, Free Tools, Bleeping Computer, 17/01/2019

Infosec (2018) Malware in Dark Web, 15/01/2018

IntSights (2018) Financial Services Threat Landscape Report, 07/2018

Ismail, N. 2018 The financial impact of data breaches is just the beginning, Information Age 8/01/2018

Kahn, R. (2018) Economic Espionage in 2017 and Beyond: 10 Shocking Ways They Are Stealing Your Intellectual Property and Corporate Mojo, Business Law Today, ABA, 19/09/2018

Kelion, L. (2017) Dark web markets boom after AlphaBay and Hansa busts, BBC, 01/08/2017

Kinder (2017), T. Hedge funds turn to dark web to gain an edge, Financial News, 02/08/2017

Krebs, B. (2015) Bidding for Breaches, Redefining Targeted Attacks, Krebs on Security, 15/09/2015

Lublin, J. (2010) How a Black Mark Can Derail a Job Search, Wall Street Journal, 02/02/2010

参考文献
つづき

Migliano, S (2018) Dark Web Market Price Index: Hacking Tools (US July 2018 Edition), 30/07/2018 MRC (2017) Global Fraud Survey, Merchant Risk Council, 07/2017

Munro, D. (2016) Healthcare’s Latest Cyber Threat: Source Code For Sale On The Dark Web, Forbes, 16/08/2016

Nadel, D. (2018) Puzzling the Internet: The Mystery of Cicada 3301, Turbofuture, 14/07/2018

Ng, A. (2018) FBI nabs hackers in theft of 15m credit cards from Chipotle, others, CNet, 01/08/2018

Nicholls, S. (2018) Police spies helped create employee ‘blacklist’ for UK companies, force admits, Euronews, 24/03/218

O’Flaherty, K. (2019) Another 127 Million Records Have Gone On Sale On The Dark Web -- Here’s What

You Should Do, Forbes, 15/02/2019

Oh, S. (2018) Why is the U.S. accusing China of stealing intellectual property?, Marketwatch, 06/04/2018

Paganini, P. (2017) MACSPY – Remote Access Trojan as a service on Dark web, Security Affairs, 14/06/2017

Palmer, D. (2018) This dark web market is dedicated to compromising your emails, ZDNet, 05/10/2018

Preston, W. (2019) Protecting Corporate Data⋯When an Employee Leaves, Druva Blog, 24/01/19

Proofpoint (2018) Drive-by as a service: BlackTDS, 13/03/2018

Raeburn, S. (2013) LinkedIn SWAM ‘blacklist’ censoring legitimate users, critics claim, The Drum, 21/08/2013

Rempfer, K. (2018) Air Force drone, Army tank documents for sale on dark web, Airforce Times, 11/07/2018

Repknight (2018) Securing the Law Firm: Dark Web footprint analysis of 500 UK legal firms, White paper, 01/2018

Schlesinger, J. & Day, A. (2018) Hackers are selling access to law firm secrets on dark web sites, CNBC, 12/07/2018

Schwartz, M. (2018) Cybercrime Markets Sell Access to Hacked Sites, Databases, Bank Info Security, 21/09/2018

Seqrite (2017) Seqrite Cyber Intelligence Labs reports breach at IRINN affecting over 6000 Indian organizations, 03/10/2017

Singh, S. (2017) Market manipulators hook onto dark web, private chats for stock tips, Times of India, 26/11/2017

Soska and Christin (2015) Measuring the Longitudinal Evolution of the Online Anonymous Marketplace Ecosystem, available at: https://www.usenix.org/system/files/conference/usenixsecurity15/sec15-paper-soska-updated.pdf

Spencer, L. (2017) Govt calls in the feds over dark web Medicare data claims, ARN, 04/07/2017 Trend Micro (2017) Access to Corporate Remote Desktops Sold for $3 in the Dark Web, Security News, 07/11/2017

UK Finance 2019a, Business Payments Survey 2019

UK Finance 2019b, Fraud the Facts 2019

参考文献
つづき

US IP Commission (2017) Update to the IP Commission Report, Commission on the Theft of American Intellectual Property

Vigliarolo, B. (2018) How to protect yourself from the Telegram-exploiting remote access Android HeroRat Trojan, TechRepublic, 02/07/2018

Wiat, A. (2018) A new generation of phishing tools was discovered In Darknet, CWIS, 02/05/2018 Wong, J. (2016) A million people now access Facebook on the “dark web” every month, 22/04/2016 Zorz, M. (2018) Access to airport’s security system sold on dark web, HelpNet Security, 11/07/2018