Computer Security Symposium 2017
23 - 25 October 2017

匿名ネットワークTorにおけるマーケット商品とセキュリティ事件との関連性に関する考察

川口　雄己[1]　山田　彰[2]　小澤　誠一[1]

概要：通常のブラウザでは検索できないダークウェブにおいて、サイバー攻撃のための商品が違法に売買されていることが問題になっている。しかしながら、ダークウェブ内のマーケットには多様な商品が売買されており、全体像の把握は難しい。本稿では、ダークウェブ内の複数のマーケットで扱われる商品を分析するシステムを開発した。このシステムは複数のマーケットから自動で製品情報を収集するクローラ部と、サイバー攻撃に関連する商品やユーザーの関心の傾向をトピックモデルと呼ばれる手法で分析する分析部で構成される。実データへの適用によりこのシステムが新たなサイバー攻撃の予測に役立つことを示した。

キーワード：CSS2017，ダークウェブ, サイバー攻撃, 機械学習, Tor クローラ, トピックモデル

A Study of Relevance between Security Incidents and Market Commodities in Anonymous Tor Network

Yuki Kawaguchi[1]　Akira yamada[2]　Ozawa seiichi[1]

Abstract: It is well known that cyberattack tools are illegally traded on *Dark Web* that is not indexed by conventional search engines. In general, it is not easy to capture trade activities on Dark Web. Obviously, to understand cyberattacks trend, there is no doubt that Dark Web is a useful information source. In this paper, we study sales trends of illegal cyberattack products on marketplaces. For this purpose, we develop an AI web-contents analyzer, which consists of Tor crawler and topic analyzer. We show that the topic analysis would be helpful for predicting new cyberattacks.

Keywords: CSS2017, Darkweb, cyberattacks, machine learning, Tor clawler, topic model

1. はじめに

2017 年 5 月にランサムウェア『WannaCry』[1] が大流行し、世界各国で取り上げられたことは記憶に新しい。同様の深刻なマルウェアによるサイバー犯罪は急激に増加しており、私たちの日常生活にも大きな影響を与えている。

よく知られているように、脆弱性を利用して攻撃を行うツールを開発する者と攻撃者は必ずしも同一ではなく、これら攻撃ツールが作成されて流通し，攻撃者の手に渡るまでには，いくつかのステップがある。一般に，ある脆弱性が発見されたあと、それを利用するためのエクスプロイットやエクスプロイットキットが登場する。そして，それらエクスプロイットを使って，より効果的かつ広範囲にサイバー攻撃を行うためのマルウェアが次々と開発されていく。これらの攻撃ツールの開発者は自ら攻撃を行うものもいるが、お金を得ることを目的として販売だけする者もいる。こうした開発者からマルウェアを手に入れた攻撃者は，各々の目的のために攻撃をしかけ、その攻撃目的は金銭を目当てにしたものから政治的，経済的目的，犯罪目的，自己満足など多岐にわたる。サイバー攻撃は，このように脆弱性の発見・流通から攻撃ツールの開発・流通といったステップを介して行われることが一般であり，実際に攻撃が観測されるまでにはいくらかの時間がかかることが多い。

[1] 神戸大学 工学研究科
Graduate School of Engineering, Kobe University
[2] KDDI 研究所
KDDI Research, Inc.

そして，これら攻撃ツールの一部は，『ダークウェブ』と呼ばれる一般のブラウザでは閲覧できないウェブ上で取引されていると言われている。

ダークウェブにアクセスするには，Tor サーキットと呼ばれる回線を利用して匿名通信を行う必要があり，これによりダークウェッブ内での行為が秘匿化され，犯罪や反社会的行為を行う者にとっては都合のよい場となっている．このため，ダークウェッブには，違法ドラッグや武器などだけでなく，マルウェアやエクスプロイットと言ったサイバー攻撃を行うツールを取り扱う闇のマーケットサイトが広がっている。よって、攻撃ツールが実際にダークウェッブでどのように取引され、攻撃者の手に渡るかについてわかれば，サイバー攻撃の動向や近い将来起こり得る攻撃に関する情報が得られる可能性がある．

本研究では，ダークウェッブの一つである Tor Hidden Service に取り扱われているサイバー攻撃関連商品の売買実態を調査する．関連研究としては，Nunes らの研究 [3] や Moore らの研究 [4] があり，前者は複数のマーケット及びフォーラムから商品情報を収集し，サイバー攻撃に関連する情報かどうかを判定する二値分類問題に帰着して商品分類器を開発した．後者の研究では、ダークウェブ内をクローラによって収集した後、いくつかのサイトに対してラベルを付与し、サポートベクトルマシン (SVM)[5] で学習することで、サイト分類器を作成した。SVM とは教師あり学習でパターン認識を行う機械学習モデルの一つであり，おもに分類問題や回帰問題に適用されてきた。以上の 2 つの研究では，教師あり学習を用いているため，分類クラスに関する正解ラベルを事前に与えてやる必要がある．しかし，闇のマーケットで取り扱われている商品数は膨大であり，一部を訓練データとして使ったとしても，ラベリングに必要なコストはかなり大きい．これに対し，本論文では，Tor 内のマーケットサイトの商品情報（値段，販売数，ベンダー信頼度など）を自動収集する Tor クローラを開発し、トピックモデルである Latent Dirichlet Allocation (LDA)[6] に収集した商品情報に適用して，クラスラベルを与えることなくマーケットの関心度の変化を捉えることのできるトピック分析モジュールを開発する．

2 節では．闇マーケットで収集する情報の種類と情報収集を行う AI ウェブコンテンツ分析システムについて述べる．3 節では，本システムを実際に 2 つの闇マーケットに適用し、得られた商品情報をトピック分析して得られた知見について述べる。

2. AI ウェブ解析システムによるモニタリング

2.1 モニタリングにより取得する情報

本研究ではまず 5 月時点でダークウェブ最大と言われていた Alphabay に注目し、情報を取得した。その後、七月初頭に管理者が逮捕され、Alphabay が閉鎖された後、

表 1 収集した商品情報.
Table 1 Extracted product information.

(1) 商品名	(2) 閲覧数
(3) 商品名	(4) 値段 (米ドル or BTC)
(5) ユーザによるコメント	(6) 販売者名
(7) カテゴリ	(8) 売上数*
(9) 発売日*	(10) 総コメント数
(11) Vendor Level	(12) Trust Level*

Alphabay に次ぐマーケットであった HansaMarket から情報を取得した。なお、HansaMarket も日本時間の 7 月 20 日に管理者が逮捕され閉鎖されている。この二つのマーケットの商品ごとに得られた情報は表 1 の通りであった、なお得られる情報は共通ではなく AlphaBay に固有の情報には※をつけている。Trust level、 Vender level はそれぞれ信頼度とどれだけ売り上げた販売者かを示しており、これらを参考にすることでマーケット利用者は詐欺などのリスクを軽減することができる。HansaMarket では Trust level や売り上げ数に該当する情報がない代わりにコメントの内訳、すなわちポジティブとネガティブなコメントの割合を見ることができ、それによって信頼できる販売者かどうか判定することができる。

2.2 AI ウェブ解析システムの概要

図 1 は，提案する AI ウェブ解析システムの構成図である．これからわかるように，提案システムは，Tor マーケットサイトのページを巡回して，商品コンテンツを自動収集する「Tor クローラ部」と、トピックモデルである LDA を使って，収集した商品情報に基づいた商品分類などを行う「トピック分析部」に分類される．Tor クローラ部は、Tor ネットワークに接続して匿名通信を行う「通信部」、サイバー攻撃に関連する商品ページの HTML を取得する「クローラ部」，表 1 に挙げた情報を HTML から JSON ファイルに抽出する「パーサ部」の 3 つに分かれる。

クロール対象としたのは、AlphaBay では Malware & Botnet，HansaMarket では Digital カテゴリの Software、Services カテゴリの Hacking と Malware である．また、Tor クローラ部の開発は「Nightmare.js」と呼ばれるオープンライブラリを用いた。このライブラリを使えば，ブラウザをプログラミングで制御することが可能であり、ログイン時に文字認証を必要とする場合でも、オペレータがブラウザ上で文字認証を行れば，Cookie の入手が可能になる。それ以後は，入手した Cookie を使って，その期限が切れるまで文字認証が不要となり，自動クロールによるページ取得が可能になる。AlphaBay では，Cookie に期限が設定されているものの，通信を行うたびに更新され、いったん Cookie を入手してクローリングを繰り返せば，実質的に完全自動化によるページ収集が可能である。

トピック分析部では，Tor クローラ部で収集された商品

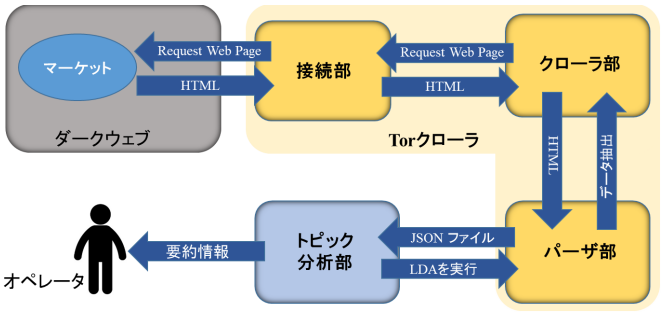

図 1 AI ウェブ解析システムの構成
Fig. 1 Architecture of proposed AI web-contents analyzer.

情報を LDA に与え，商品のカテゴリ分類 (トピック分類) が行われる．各トピックは，それぞれを代表する単語の集合で与えられ、オペレータはその単語分布を確認することで、各トピックが表している商品情報の傾向をつかむことができる．LDA の実行にはクラスラベルが不要であり，AI ウェブ解析システムは教師なしで商品の分類情報を学習できる．

3. 闇マーケットの商品分析

本節では，ダークウェブで最大のマーケットに分類される AlphaBay と HansaMarket をターゲットとして，その商品情報の解析結果を考察する。

3.1 人気商品の分析

本節ではマーケットサイトで販売されていた商品のうち 6 月 7 日〜13 日、6 月 14 日〜20 日のそれぞれの期間で商品の売り上げの増加が大きかったものに注目し、分析を行う。

3.1.1 調査方法

人気順ソート、新着ソートともに 6 月 7 日〜13 日、6 月 14 日〜20 日のそれぞれの期間で一日あたり 2250 件ずつ収集し、そのうち商品の売り上げの増加が大きかったもの上位 10 件ずつに注目し、分析を行う。

3.1.2 調査結果

表 2 と表 3 に売り上げ上位商品を示す。なお、商品名は見やすさのため、元データに含まれていた煽り文などを排除し、できる限り商品名のみを表示した。表から、売り上げ上位の商品でも売り上げが二桁のものが多く、大規模に売れている商品は多くないことがわかる。また、6 月 7 日〜13 日の期間で非常に多くの数を売り上げている Hack であるが、表 3 の売り上げトップの商品と同一である。これは商品説明にも hack としか書かれておらず、詳細がわからないばかりか、はじめ The complete hacking course という商品名だったものが 6/12 日に Hack に代わり、その後一日で 1000 件以上を売り上げるという不審な挙動を見せ、さらに 6 月 14 日には商品名が Bypass Account Verification に変わり、商品説明が加わった。その後も 6 月 17 日には 2017 Ultimate Bank Cashout Guide という商品名に変更されており、公開されているフィードバックも存在していない。商品詳細が分からない時点で驚異的な売り上げがあったことからなんらかの改ざんあるいは不正行為を働く販売者である。または、アカウント乗っ取りなどの被害を受け、クラッカーが自らの行為を誇示するために、商品情報を hack に書き換えた可能性が高い。全体としてみると安価な商品が多く、表 2 の Jabber Spammer 以外は最新とは言えない商品であるが売れている。このことから、効果が信頼できる商品が売れやすい傾向にあることがわかる。本来マルウェアとしては最新の脆弱性を利用したものが活発に取引されやすいと考えられるが、実際には効果が信頼できる商品が優先されている。

3.2 販売者の傾向

本節では、販売者の trust level と 0 ドル商品を販売していることの間に相関が存在するか考察する。

3.2.1 調査方法

6 月 7 日〜20 日までの各ソートの上位 750 件の商品を販売している販売者を対象にそれぞれの trust level、と 0 ドルの商品の販売との間に相関が存在するかを確かめた。

3.2.2 結果

図 2 に level ごとの 0 ドル商品販売者の割合を示す。マルウェア商品を販売する 166 人の販売者のうち 73 人が 0 ドル商品を販売しており、半数近くの販売者が無料の商品を提供していることや低レベル層での販売が多いことがわかる。レベルの低い販売者はこれからのレベル上昇のために、レベルの高い販売者は 0 ドル商品を販売したことによって現在のレベルを手に入れていると考えられる。また無料の商品は昔から存在するものが多いと考えられ、例えば表 2 の Zeus は 2007 年から確認されているボットネットである。

3.3 WannaCry

WannaCry とは感染した PC のデータを暗号化し、使用不能にしたのち、暗号化を解除することと引き換えに “ 身

表 2 売り上げ上位 (6 月 7 日〜13 日)
Table 2 Top sales (6/7-6/13)

Name	Release Date	Price (USD)	Sales/Week	Trust Level
Hack	May 26, 2017	0.00	1120	4
Jabber Spammer	May 10, 2017	10.00	125	3
Super cheap fullz	Apr 17, 2015	0.88	32	7
Allways encrypt and stay safe in cyberspace PGP	Oct 29, 2015	0.00	27	6
Wifi Automated Cracker	Jan 16, 2016	0.98	25	7
Bitcoin Stealer	Nov 4, 2016	0.00	20	4
Super Bluetooth Hack Phones	Jan 14, 2016	0.99	18	7
Free 230517 Update Aegiscrypter 9.5	Dec 8 2016	0.00	16	4
BlackShades RAT 5.5.1	Jul 11 2015	1.10	15	7
Free 230517 Update Zeus 3.0.1	May 8 2017	0.00	14	4

表 3 売り上げ上位 (6 月 14 日〜20 日)
Table 3 Top sales (6/14-6/20)

Name	Release Date	Price (USD)	Sales/Week	Trust Level
2017 Ultimate Bank Cashout Guide	May 26, 2017	0.00	36	4
Allways encrypt and stay safe in cyberspace PGP	Oct 29 2015	0.00	18	6
SGCorp CoinGrab	Jun 8 2017	25.00	15	3
BlackShades RAT 5.5.1	Jul 11 2015	1.10	14	7
FREE 230517 Update Loki 1.6	May 8 2017	0.00	14	4
FREE 230517 Update Cyborg v3.9.2	Dec 8 2016	0.00	14	4
Rent Botnet Flat Rate	Oct 25 2016	50.00	13	5
Super cheap fullz	Apr 17 2015	0.88	12	7
Bitcoin Stealer	Nov 4 2016	0.00	12	4
Free SpyNote	Mar 5 2017	0.00	10	7

代金 ” を要求するランサムウェアの一種であり、2017 年 5 月に世界で大規模な感染を見せた。これには Eternalblue と呼ばれるエクスプロイトが使用され、wannaCry の流行後同様の exploit を用いた UIWIX,EternalRocks,Adykuzz などのマルウェアが相次いで流行した。本項では世界各国でおおきな騒ぎとなったマルウェア、WannCry であるが、表の世界だけではなく、ダークウェブのマーケットに対しても影響を及ぼしていたか調査を行った。

3.3.1 調査方法

WannaCry が世界で確認された 5 月 12 日前後に AlphaBay で販売されていたランサムウェア商品の閲覧数及び販売数を調べることでダークウェブの利用者の興味を変遷を調査した。クローラで収集した範囲は各ソート一日 60 件ずつである。追跡した商品は表 4 に記載した。なお同名、同ベンダーの商品が存在した場合最新版を追跡した。

3.3.2 結果

1 日あたりの閲覧数の推移のグラフを図 3 に示す。図中において Blackmail Bitcoin Ransomware が図中で途切れているのはそこでクローラの収集範囲を外れたためである。

図 3 より WannaCry が大規模に活動を開始した 5/12 日の後、大幅な増加が見られると考えられたが、実際には stampado2 以外の商品はほとんど単調増加に近く、有意な差は発見できなかった。また、販売数であるがこれもまた期間中に stampado2 以外の商品は一件も売れていなかった。唯一有意な差が確認できた stampado2、Stampado は 2016 年半ばに確認されたランサムウェアであり、新しいランサムウェアではない。にもかかわらず stampado2 にのみ影響が確認されたことから、3.1 節の結果に加えて、ここでもマーケットの利用者は機能が信頼できる商品を優先する傾向がある。

3.4 人気商品の説明文に対する LDA の適用

Latent Dirichlet Allication(LDA) [6] とは Blei らによって考案された文書などの隠れた構造をもったデータ集合のなかからその隠れた構造を見つけ出すことができる解析手法であり主に自然言語処理の分野で利用されている．文書に適用する場合、同じ文書のなかには現れやすい語彙の集合（＝トピック）が存在し、トピックモデルを使うことでこのようなトピックを抽出することができる。商品の解析に LDA を用いる利点として、まず教師なし学習である点があげられる。LDA ではモデルの学習の際に教師データを必要としない、そのため、多種多様な商品それぞれに対してラベル付けをすることが難しいダークウェブマーケットに対して有効であると言える。また、単純に単語の出現頻度のみの分析との違いとして、単語同士の共起関係に注目していることがあげられる。例えば表 5 の 6/7-6/13 期間の Topic1 では bot と windows が同トピックに存在することから、Windows を対象とするボットネットが人気が

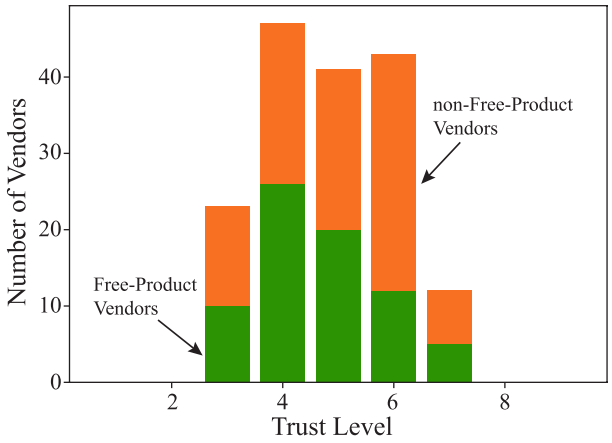

図 2 trust level ごとの 0 ドル商品販売者の割合

Fig. 2 Percentage of free products seller per trust level

表 4 ランサムウェア

Table 4 Ransomwares

Name	Release Date	Price (USD)
Stampado 2	Jul 12, 2016	39.00
Blackmail Bitcoin Ransomware	May 1, 2017	0.00
Best Blackmail Bitcoin Ransomware 2017	May 7, 2017	0.00
BTC Ransomware	May 9, 2017	0.00
Load for Your Botnet - Ransomware - Bank Bot - ClickBot/	May 9, 2017	20.00
The Underground Collection	May 11, 2017	0.00
Philadelphia Ransomware	May 15, 2017	29.00

あることなどが予測できる。実際に表 2 に存在する Zeus ボットネットは windows で動作するボットネットである。また教師なし学習である利点として、本システムを OSINT として活用することを考えた場合、OSINT 利用者に対してラベル付けの必要なしに、自動的に LDA の結果を提供することができる。

3.4.1 評価方法

まず、AlphaBay において Botnet&Malware カテゴリから人気順ソート、新着ソート合わせて 1500 件収集した商品のうち 6 月 7 日〜13 日、6 月 14 日〜20 日のそれぞれの期間で商品の売り上げの増加が大きかったもの上位 100 件ずつに対して LDA を適用、その説明文から Topic 数 5 でトピックを抽出し、変化に着目した。次に、AlphaBay が閉鎖する最後の一週間と HansaMarket が閉鎖するまでの一週間の閲覧数上位のサイバー攻撃関連の商品 100 件ずつに適用する。得られた一週間の Topic を比較し、各マーケットの違いがあるかを考察する。

3.4.2 AlphaBay に対する適用結果

表 5 に抽出したトピックの代表単語を示す。Topic4 に着目すると 6/14-6/20 の期間では新たに antidetect や carding といった単語が出現しており、探知されない不正な金銭取引を行うマルウェアの需要が高まっていることがわかる。実際表 3 にも fully undetectable をキャッチコピーとする不正に bitcoin を盗むマルウェアである SGCorp CoinGrab が出現していることがわかる。このように LDA を利用することで全ての商品の情報を見ることなく、全体の商品の傾向の変化を確認できると考えられる。

3.4.3 AlphaBay と HansaMarket の傾向

各マーケットから得られた商品のトピックおよび、各トピックが最も多く割合を示す商品上位二つを表 6,7 に示す。トピック 1,2,3 ではどちらのマーケットでも非常に似通ったトピックが出現していることがわかる。実際売られている商品にも同名の商品が多く存在しており、例えば Get Access To Any Phone Bypass Passcode という商品は表 6 のトピック 3、表 7 のトピック 4 の双方に出現している。ほかにも 3.3 で登場した Blackmail Bitcoin Ransomware も HansaMarket でも複数の販売者により販売されており共通する人気商品は少なくない。しかしながら販売者の多くが共通しているかというとそうではない可能性がある。もし、AlphaBay でも販売を行っており、一定の実績を持つ販売者が HansaMarket に移入したのであれば、その信頼性を HansaMarket でも使うため、同販売者であることを示す可能性が高い。モニタリング期間中サイバー関連商品を販売していた販売者は AlphaBay で 166 人、HansaMarket では 97 人が確認されたが両マーケットに共通する名前を用いていた販売者は 21 人であった。これは AlphaBay 閉鎖後 HansaMarket では登録者が殺到したため、新規登録を一時停止していたこともあり、AlphaBay 閉鎖後に移動

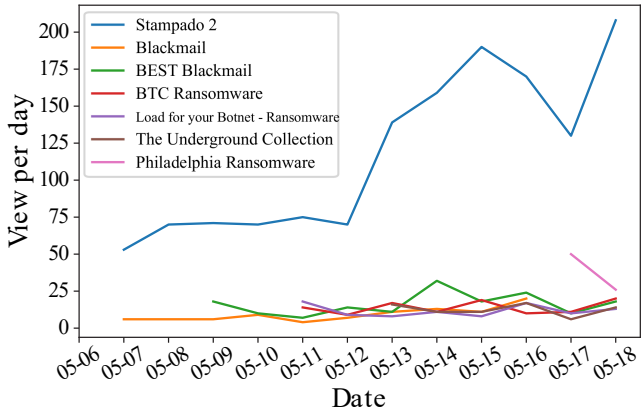

図 3 一日当たりの閲覧数
Fig. 3 The number of views per day.

表 5 AlphaBay におけるトピックの変化
Table 5 Change of topics in AlphaBay

Topic	6/7-6/13	6/14-6/20
1	Account Login VPN Hacking PayPal Bank Pass Premium Money Bitcoin	Account Hacking Course Premium Pass VPN Accounts Fraud Money Phone
2	File Bot http Windows php anti Use Files User Network	com Password Windows File Files Http Bot Attack Advanced Computer
3	Bitcoin Carding Free Victim Cc PayPal Guide Cashout BTC Money	Account Login PayPal Bitcoin Cashout BTC Cc Bank Guide Carding
4	com Tools http Make Time Money Pass Bank Premium Account	**Antidetect** Program Software Use **Carding** http Crack Windows **Fraud** Internet
5	Password Recovery Crack Advanced Hack Passwords Forensic Phone Tools Hacking	Accounts Phone Want Crack Support Android New Make Software Hack

できていない販売者がいたことも考えられる。

4. 結論

本稿では、ダークウェブにおける最大のマーケットサイトであった AlphaBay や HansaMarket で流通している商品に対して、LDA によるトピ?ック分類を行い、ユーザの関心の変化や人気商品の傾向を分析した。その結果、次のようなことがわかった。

- マーケット利用者は、新しさよりも信頼度を重視して商品を購入する。
- LDA によってマーケットで取引される商品傾向を効率的に観測できる。

今回のシステムを開発した最終的な目的の一つに、収集した情報に対する OSINT(Open Source INTelligence) の活用がある。OSINT とはその名の通り、公開情報を利用し知見を獲得する手法であり、近年セキュリティの分野でも注目を集めている。OSINT にはいわゆるセキュリティ関連のブログやレポート、SNS の投稿などが含まれている。本研究ではダークウェブからサイバー攻撃に関する情報を取得してきたが、これまで収集してきた情報にこれらの表層ウェブの情報を活用することでサイバー攻撃に関する情報を多角的に解析することが可能になると考えている。

謝辞

本研究は，独立行政法人情報通信研究機構（NICT）の委託研究および JSPS 科研費 16H02874 の助成を受けたものです。

参考文献

[1] Goodin, D., “NSA backdoor detected on 55,000 Windows boxes can now be remotely removed,” https://arstechnica.com/security/2017/04/nsa-backdoor-detected-on-55000-windows-boxes-can-now-be-remotely-removed/ ARS Technica.
[2] McCoy, D., Bauer, K., Grunwald, D., Kohno, T., Sicker, D., “Shining light in dark places: Understanding the Tor network,” in Borisov, N., Goldberg, I. (Eds.), *Privacy Enhancing Technologies: 8th International Symposium, PETS 2008*, LNCS, vol. 5134. pp. 63–76 (2008)
[3] Nunes, E., et al. “Darknet and deepnet mining for proactive cybersecurity threat intelligence,” *IEEE Conference on.Intelligence and Security Informatics*, pp. 7–12 (2016)
[4] Moore, D., Thomas R., “Cryptopolitik and the Darknet.” Survival, vol. 58, no. 1, pp. 7–38 (2016)
[5] Cortes, C.,Vapnik, V., “Support-vector networks,” *Machine Learning*. Vol. 20, No. 3, pp. 273?297, 1995.
[6] Blei, D. M., Ng, A. Y., Jordan, Mm I., “Latent dirichlet allocation,” *Journal of Machine Learning Research*, vol. 3, pp. 993–1022 (2003)
[7] Van Buskirk, J., Naicker, S., Bruno, R. B., Breen, C.,

表 6 AlphaBay のトピックと代表商品

Table 6 AlphaBay's topics and representative products

Topic	代表単語	代表商品
1	Carding Software Money Free Bitcoin Need BTC Guide Bank PayPal	BTC Stealer 4.3 and Mass Address Generator 1.2+, Professional Carding Software
2	File Files Advanced Hacking Computer Use Ransomware Network Victim Windows	Advanced System Protector, KilerRat v10.0.0 Full
3	Account Login PayPal Hacking Bitcoin VPN Cashout Bank Cc BTC	VPN Account For Life ironsocket.com, Bitcoin Stealer
4	Password Com Hack Recovery Phone WWW Forensic Passwords Accounts Software	Get Access to Any Phone Bypass Passcodes Retrieve All the Data on the Phone, Professional Phone Hack software
5	http php ID Exploit Time Make Money Tools File Use	Voice changer (Android, Windows), Silent Exploit Setup Service

表 7 HansaMarket のトピックと代表商品

Table 7 HansaMarket's topics and representative products

Topic	AlphaBay	HansaMarket
1	Carding Money Guide Method Make PayPal Cashout Free Tutorial Cc	All in One-Carding/Money Making/Hacking, Overnight Money Making Machine!
2	Windows Computer Hacking Software Guide Security Files Use Internet Network	Bugtroid - Android Mega Tools Pack, Diamond Rat
3	Account Login Cashout PayPal Bitcoin Hacking Bank VPN BTC ebay	Get Access To Any Phone Bypass Passcode, Account Hacking Program
4	Stealer Phone Email Time Access BTC Password Bitcoin Com Use	True Online Anonymity Kit, True Online Anonymity Kit
5	Black Super Hash Fast Double High New Easy Original Ultimate	Traffic Encraser Include Atomic Email Sender and Other Tools for Facebook, Backlink, Keyw, DK Brute - Bruteforce RDP, SSH, SMB, pop3, pop3s, VNC, FTP

Roxburgh, A., "Drugs and the Internet," (2016)
[8] Steven N., "Buying drugs online remains easy, 2 years after FBI killed Silk Road," https://www.usnews.com/news/articles/2015/10/02/buying-drugs-online-remains-easy-2-years-after-fbi-killed-silk-road (Oct. 2, 2015)
[9] "shodan" https://www.shodan.io/