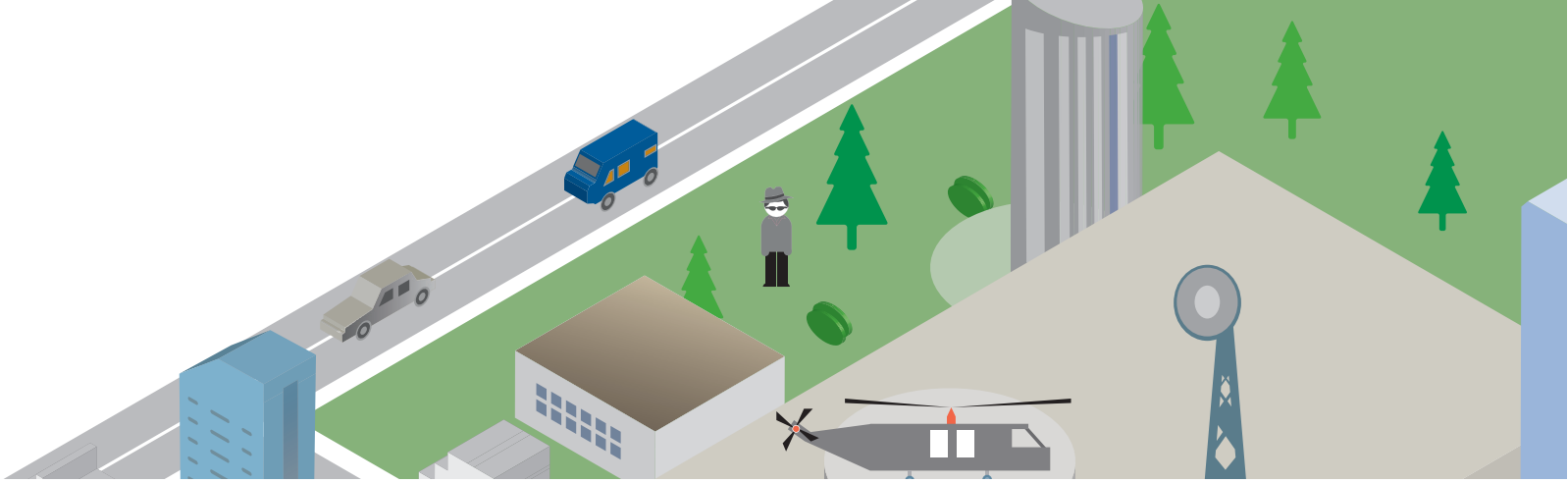
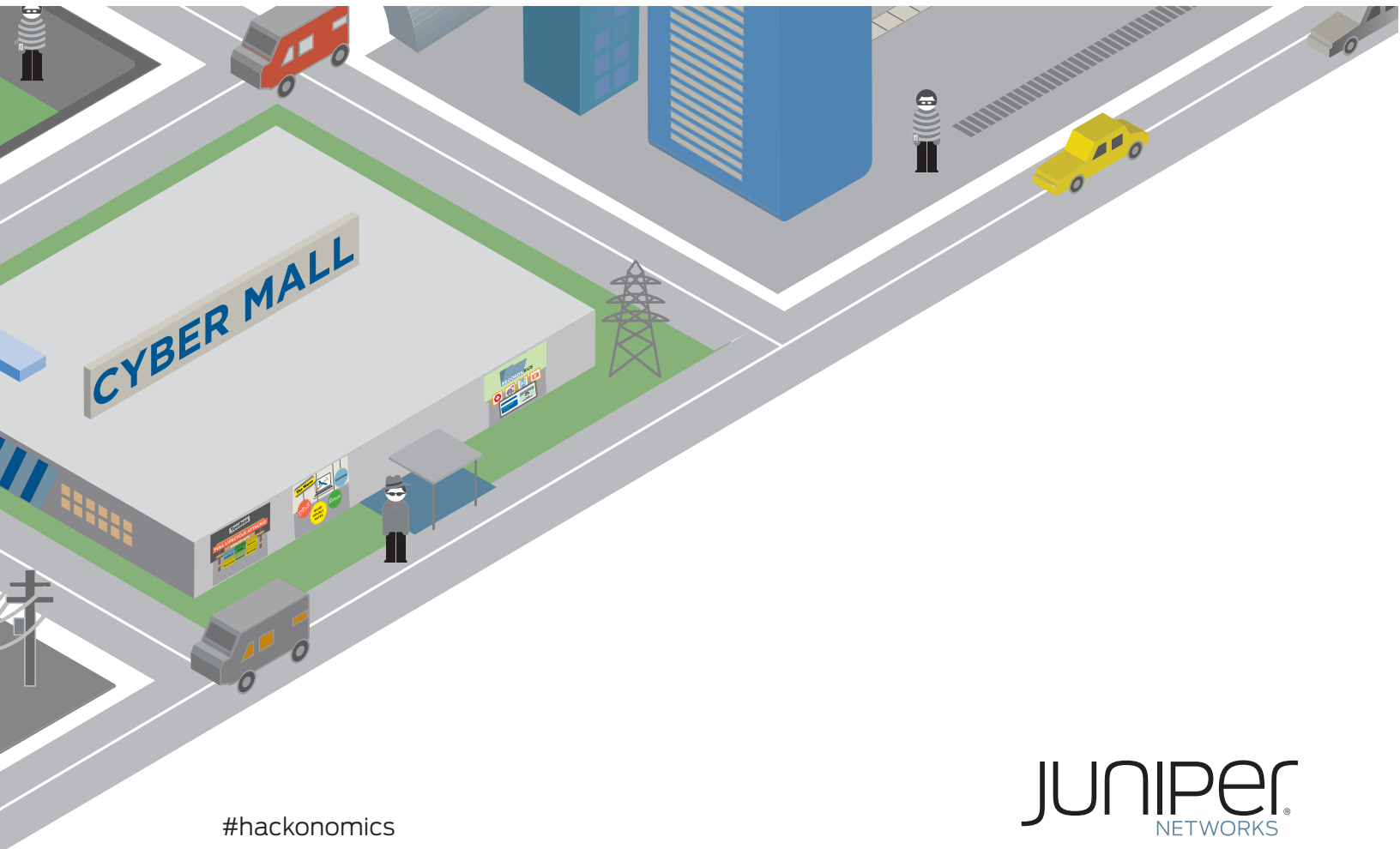




「アンダーグラウンド」から「成熟した大都市」へ サイバー闇市場の経済分析

ランド研究所の調査に対するジュニパーネットワークスの見解



#hackonomics

JUNIPER[®]
NETWORKS

個人情報情報を標的としたサイバー攻撃は毎日のように発生していますが、それはなぜでしょうか？

ランド研究所の調査に対するジュニパーネットワークスの見解

企業へのサイバー攻撃は、知的財産やブランド評価を危険にさらすと同時に対策コストはますます増加しています。過去10年の間に、サイバー犯罪、ハッキングツール、および闇市場からまったく新しい経済が生み出されました。

サイバー犯罪の世界は根深く複雑で、高度に成熟した市場経済になっています。ジュニパーネットワークスの後援により、ランド研究所が発表した最新の報告書「Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar」には、こうした闇市場の仕組み、成り立ち、過去のトレンド、今後の見通しについての分析が示されています。

この闇市場は「サイバー・アンダーグラウンド」と呼ばれることもありますが、ジュニパーネットワークスは「成熟した大都市」と表現するのが現代においてはより相応しいと考えています。



これまでの調査で、ハッカーの闇市場が及ぼす影響を金額で数値化する試みはありましたが、経済的構造、成熟度、それによって企業や政府機関に及ぼされる影響を分析する調査は今までありませんでした。

今回の調査にあたりランド研究所は、学術機関の研究者、セキュリティ研究者、記者、セキュリティベンダー、法執行機関など、この闇市場に現在または過去に携わっていた世界的な専門家に対する綿密なインタビューを実施しました。ジュニパーネットワークスが持つネットワーク・セキュリティ・エコシステムにおける幅広い経験からも裏付けられますが、ランド研究所の調査によると、サイバー闇市場は、成熟かつ成長を続ける堅牢なインフラおよび社会組織を持つ数十億ドル規模の経済に匹敵する市場となっています。

成熟した市場

ランド研究所は、サイバー闇市場の進化は、革新と成長を伴う自由市場の進化を反映したものであると報告しています。本調査においてランド研究所は、闇経済の成熟度を示す5つの重要な指標を見いだしました。



1. 高度化

サイバー闇市場の仕組みや、売買されているツールおよび攻撃のタイプは、非常に高度化しており、最新のニーズに応じて変化し、適応しています。



2. 専門化

サイバー闇市場には、他とは全く異なるカスタマイズされた商品、場所、役割分担があり、明確な階層社会が存在します。そこは上位の立場にある者がより多くの利益を手に入れる社会なのです。



3. 信頼性

サイバー闇市場の参加者や商品は、自己申告通りの参加者や商品である場合がほとんどですが、中には他人をだまそうとしたり売り手の利益のために不要な機能を加えようとする者が必ずいます。時間が経つにつれ、優れた商品が粗悪な商品を淘汰し、高品質なブランドがプレミアム価格を請求できるようになります。今回の調査で、ベンダーによっては商品の寿命や価値を保証したり、顧客による商品使用状況を追跡することでハッカー版の「デジタル著作権」管理を行っていたりするベンダーも存在することが新たに分かりました。



4. アクセシビリティ

サイバー闇市場への参入コストは低く、ある程度簡単に携わることが出来ます。ネット上のフォーラムや電子市場は、ハッカーを目指す者にとってエントリーポイントの役割を果たしています。ただし最近の傾向では、より多くの取引が、信頼性があり検査された確実なパートナーとの間で秘密裏に行われています。



5. 回復力

通常であれば市場を崩壊させるような外的な出来事が起きても、サイバー闇市場は実際に影響を受けることはなく、仮に受けたとしても回復しています。資金調達から多くのハッカーが利用する市場まで、サイバー闇市場のあらゆる部分を崩壊させ停止させるために、法執行機関が取り組みを改善、強化していますが、ハッカー経済は極めて回復力が高いことが実証されています。攻撃に対する需要や潜在的利益が高すぎるのが大きな要因となっています。

成熟した大都市

ジュニパーネットワークスでは、ハッカー経済をサイバー・アンダーグラウンドと捉えるよりも、多様なコミュニティ、業界、および交流がある「成熟した大都市」と見る方が相応しいと考えています。かつてのハッカー市場が、エゴや知名度といった動機を持つ個人による孤立した臨時的なネットワークから成り立つ多種多様な世界であったのに対し、今や金銭を目的として高度に組織化され、洗練された集団の活動の場となっていると、ランド研究所は強く主張しています。

大都市と同じように、闇市場には、供給者（熟練者および未経験者）、ベンダー、潜在的購入者、およびデジタルベースの犯罪にまつわる商品やサービスの仲介者が集まっています。

店頭での販売

eコマースの他の形態と同様、多数のデータレコード、エクスプロイトキット、および商品が店頭で売買されています。これには、インスタント・メッセージング・チャットのチャネル、フォーラムから、洗練された店舗まで、あらゆるものが含まれます。それらの中には海外拠点を持ち、数億ドルもの収益をあげる7～8万人規模の組織も存在することが明らかになりました。

サービス形態での販売

ハッカー経済では商品だけでなく攻撃サービスも購入可能です。ボットネットの急増により、犯罪者は他の犯罪者にDDoS攻撃やスパムをサービスとして販売できるようになりました。実際、攻撃の足掛かりとなるエクスプロイトキットは通常、1週間または1カ月単位で「貸し出し」されるのが一般的です。納税手続きのために支払いをしたり、オンラインの納税サービス（従来のSaaSモデル）を使用したりするのと同じように、現在サイバー闇市場でも同様の支払いサービスが数多く提供されています。

階層社会

合法的なビジネスと同じように、サイバー闇市場の世界において上位へ上り詰めるには、コネクションと人間関係が重要になることが分かりました。トップに上るには個人的なコネが必要で、上位層に君臨する者が最大の利益を手に入れています。



成熟した大都市

通貨

サイバー闇市場の取引は多くの場合、デジタル通貨を用いて行われます。ランド研究所が分析で取り上げた例として、ビットコイン、Pecunix、AlertPay、PPcoin、Litecoin、Feathercoin、ビットコインを拡張したゼロコインなどがあります。デジタル通貨以外の方法で取引が行われることもありますが、多くの犯罪サイトが匿名性とセキュリティを重視し、デジタル専用通貨以外は受け付けないようになり始めていることが判明しました。

法の原則

ハッカーの間にも道徳規範があります。サイバー闇市場の多くの部分はきちんと組織化され、法律のようなルールにより監視されています。しかも、市場参加者を欺くような行為は原則として禁じられており、違反するとその市場から締め出されます。また、サイバー犯罪の上位層へ上り詰めるほど、参加するにあたっては詳細な審査のプロセスがあります。

犯罪

サイバー闇市場においても犯罪が起きており、その中でも請求された商品またはサービスを提供しない特に悪質な犯罪者たちは「リップパー」と呼ばれています。



成熟した大都市

教育とトレーニング

ランド研究所の調査により、サイバー犯罪に関する幅広いツールや資料が入手可能であることが分かりました。例えばYouTubeのビデオやGoogleのガイドを使って、ハッカーはエクスプロイトキットの使用方法やクレジットカードの入手方法を学ぶことができます。このようなすぐに使える教材は、ハッカー経済への参入を容易にする原因にもなっています。ランド研究所の報告書は、こうした教材へのアクセスをデジタルに慣れ親しんだ世代が利用することで犯罪の高度化が進み、管理者、専門家、ベンダー、一般メンバーなど、ハッカー経済内により多くの役割を生むと指摘しています。

多様性

中国、中南米、東欧からのサイバー犯罪はマルウェア攻撃の数の多さで知られていますが、質の高さではロシアがトップであると認識されていることが分かりました。また、国ごとに得意な領域や関心の高い領域が異なることも明らかになっています。例えば、多くのベトナム人犯罪グループは、主としてeコマースのハッキングを行っています。ロシア、ルーマニア、リトアニア、ウクライナのサイバー犯罪は、金融機関を標的にしています。中国のサイバー犯罪の多くは、知的財産に特化しています。米国ベースのサイバー犯罪の多くは、米国を拠点とする金融システムを標的にしています。ランド研究所の調査により、サイバー犯罪の多様性に加え、こうしたグループ間での相互交流がまだかつてないほど増えていることも新たに判明しました。



ジュニパーネットワークスの視点：サイバー攻撃の阻止および防御

以上のことから、ハッカーの闇市場の成熟が進むことにより、企業や個人は新たに重要な課題に直面しているといえます。報告書は、攻撃する能力が防御する能力を上回る可能性が高いと示しているのです。これは、企業や個人の情報を保護する責任がある人々にとって何を意味しているのでしょうか。

ジュニパーネットワークスは、サイバー犯罪市場の成長が加速した背景にある根本的な原因、つまり成功を後押ししている経済そのものを調べる必要がある、と考えています。

ハッキングの経済を変え、攻撃を実現可能にしているバリューチェーンを破壊する方法を探さなければなりません。

そのためにはどうすべきでしょうか。こちらから攻撃したり、反撃したりすることはできません。それでは、我々のモラルを問われることになるでしょう。たとえ違法なことをしなくても、受け身の状態から脱却することはできます。侵入偽装テクノロジーを使用するなど、積極的な防御体制を敷くことで、攻撃者を特定し、阻止し、妨げることは、サイバー犯罪に対して確実かつ素晴らしい方法となります。

例えば、犯罪者の時間を無駄にしたり、犯罪者が闇市場で購入したエクスプロイトツールを無効化したりすることができれば、情報漏えいを防ぎ、攻撃サイクルの早い段階でバリューチェーンを断ち切ることができます。また、タールトラップとして偽のデータやハッキングフォーラムを挿入し、サイバー犯罪者同士の間において不信を招くことで、市場を攪乱させることもできます。あるいは、悪玉ハッカーに正規のセキュリティ研究者になることを奨励するために経済的インセンティブを用意するという方法もあります。

様々な対策が考えられる中、現状において明確なことが1つあります。それは、企業がいかにしてより積極的にサイバー空間で自身を防御できるかについて、セキュリティ業界、政府、および政府機関が協力して新たな基準を確立すると同時に、プライバシー、市民の自由、および公的機関と民間企業の活動の適切な境界を尊重する必要があるということです。

最終的にどのような対策を講じるにしても、攻撃者やそのシステムと動機を理解することは、業界においてより優れた防御対策の提供を検討する上で役立つはずです。

今回の調査「Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar」は、ランド研究所が2013年10月から12月にかけて実施した、学術機関の研究者、セキュリティ研究者、記者、セキュリティベンダー、法執行機関など、この闇市場に現在または過去に携わっていた世界的な専門家に対する綿密なインタビューに基づいています。ジュニパーネットワークスの後援によるランド研究所の調査は今回が初めてとなります。

Corporate and Sales Headquarters

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or +1.408.745.2000
Fax: +1.408.745.2100
www.juniper.net

APAC and EMEA Headquarters

Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Amsterdam, The Netherlands
Phone: +31.0.207.125.700
Fax: +31.0.207.125.701

Copyright 2014 Juniper Networks, Inc. All rights reserved. Juniper Networks and the Juniper Networks logo are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners. Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.



Juniper Networks is in the business of network innovation. From devices to data centers, from consumers to cloud providers, Juniper Networks delivers the software, silicon and systems that transform the experience and economics of networking. The company serves customers and partners worldwide. Additional information can be found at www.juniper.net.