アンダーグラウンドのハッカー市場動向調査の結果レポート

～安価な不正商品とサービスの氾濫により、専門知識がなくとも様々な犯罪が可能な実態が明らかに～

アンダーグラウンドのハッカー市場が急速に拡大

2013 年のハッカー市場と比べてもっとも大きな違いは、新しい身分証明書キット、パスポート、公共料金の請求書、社会保障カード、運転免許証など、詐欺に利用される偽造文書の流通により市場が急速に拡大する傾向にあることです。この種の文書を偽造するには、実際にオフラインで詐欺を働く必要があります。これには、複製したクレジットカードやデビットカードを使って小売店で高級な商品を購入することをはじめ、銀行ローンを申請したり、小切手詐欺を行ったり、政府関連の詐欺を試みたりすることが含まれます。

2014 年のアンダーグラウンド市場で特に目立ったその他の製品は次のようなものがあります。

- **ハッキングのチュートリアル**: ハッカーは自らが犯罪行為を行うことで収入を得ているだけでなく、そのノウハウを商品として販売し、少額の追加収入獲得にも手を広げるようになってきています。

- **プレミアムクレジットカードを販売するハッカーの数**: 2014 年はサイバー侵害が多く、数百万枚のクレジットカードおよびデビットカードの情報漏洩が報告されています。そのため、闇の市場にプレミアムクレジットカードが大量に出回る可能性が高いことが懸念されます。

- **闇市場でも顧客満足度向上が成功のカギ**: 合法で健全な表の市場と同様に、製品やサービスを販売する様々なベンダーが集まる闇市場においても、顧客間のベンダーに対する評判がビジネスを成功させるために重要な指標になっています。販売している盗難データに対して、「迅速なカスタマサービス」と「100 %保証」を提供することで差別化を図るベンダーも登場しています。闇市場で暗躍するベンダーは、彼らの顧客がオンラインまたはオフラインでの詐欺を成功させられるように、販売するツールやサービスの継続的な強化に取り組んでいます。合法な市場においては"企業努力"と見なされるこのような行為も、犯罪を増加させうる脅威です。

販売されている偽造の資格情報:

身分証明書、パスポート、運転免許証、社会保障カード

アンダーグラウンドのハッカー市場において最も注目すべき変化の 1 つは、販売されている偽造の資格情報の数です。これには、新しい身分証明書のパッケージ、パスポート、運転免許証、社会保障カードなどが含まれます。 これらの証明文書は、銀行ローンの申請や小切手およびクレジットカード詐欺、政府援助詐欺、医療詐欺などのなりすまし詐欺を実行する上で必要なツールです。

- **販売されている新しい身分証明書**: 新しい身分証明書を求める場合、実際に使用されている社会保障カードのスキャンと名前および住所を 250ドルで購入することができます。さらに100ドル支払えば、追加

で身分確認のための公共料金請求書が付きます。この実例は、ハッカーがあらゆる種類のデータを収益化していることを示しており、銀行、小売店、医療業界だけでなく、公共施設業界も個人を特定できる情報（PII）のターゲットであることを物語っています。これらの資格情報および対応する運転免許証があれば、詐欺で政府援助プログラムに応募したり、その他の犯罪行為（銀行およびクレジットカード詐欺、医療詐欺）を行ったりすることができます。

- **偽造パスポート**: 米国以外の偽造パスポートは 200～500 ドルで取引されています。買い手は住所、本籍、年齢などの詳細情報が記載されたパスポートのスキャンを入手できます。 ほとんどのビジネスでは、相手の身分証明としてパスポートのスキャンが通用するだけでなく、クレジットカード詐欺、小切手詐欺、政府援助詐欺など多様な詐欺に利用できます。

  注 米国のパスポートは、アンダーグラウンドのハッカー市場で広く利用されませんでした。

- **偽造運転免許証**: 米国ベースの運転免許証は 1 枚当たり 100～150 ドル支払えば、任意の名前、住所、州などの情報でカスタマイズしながら偽造することができます。ハッカーは、免許証に入っているホログラムも偽造しています。大量に購入する場合は 1 枚あたりの価格は下がります。 偽造運転免許証は、小切手詐欺やクレジットカード詐欺など多くの種類の詐欺に使われています。
  - 2014 年 9 月、米国の法執行機関は、偽造運転免許証を作成および販売していた 3 人の詐欺犯を逮捕しました。これらは、不正現金引出を目的として使用されたと米連邦捜査局(FBI)から報告されています。ハッキングや ATM スキミングによって入手した盗難クレジットカード情報などが偽造クレジットカードにエンコードされ、被害者の口座から現金を盗むために使用されました。FBI によれば、2013 年 12 月 30 日から 2014 年 6 月 23 日までに、共謀者が偽造運転免許証を 1,514 枚販売し、232,660 ドルを得ていました。

- **偽造社会保障カード**: 被害者の名前、住所、および社会保障番号を既に購入していて、対応する社会保障カードも入手したい場合、カードは平均して 250～400 ドルで買い求めることが可能です。偽造パスポートと同様に、詐欺犯は社会保障カードのスキャンを提供します。 偽造カードを使用すると、不正に税の還付申告を受けたり、さまざまな金融口座を開いたりすることができます。

販売されているプレミアムクレジットカード:

プラチナ/ゴールド/プレステージ/ブラックなど、カード種類と国を指定して購入可能

非常に多くのハッカー市場で、各国のプレミアムクレジットカード（プラチナ、ゴールド、ブラック、プレステージなど）や、スタンダードのクレジットカードの販売（Track I および Track II データを含む）の広告が出されています。 特に、米国、カナダ、英国、欧州、ブラジル、アルゼンチン、およびグルジアから盗まれたクレジットカードが多く出品されています。

- あるサイトでは、Track I および II データを含むプレミアムおよびゴールドのマスターカードを 35ドル/枚で、Track I および II データを含む米国以外のスタンダードのマスターカードを 17ドル/枚、プレミアム Visa カードは 23 ドルで販売されていました。
- これと同じアンダーグラウンドなウェブサイトで、14,000,000 枚の米国のクレジットカード、294,000 枚のブラジルのクレジットカード、342,179 枚の世界のクレジットカード、212,100 枚のカナダのクレジットカード、75,992 枚の英国のクレジットカード、26,873 枚の EU のクレジットカードの販売が確認されています。

大量販売されるプレミアムクレジットカードの価格例（Track I および II データ含まず）:

- 10 枚　　13 ドル/枚
- 50 枚　　12 ドル/枚
- 100 枚　　11.50 ドル/枚
- 500 枚　　11 ドル/枚
- 1000 枚　　10 ドル/枚（人気のあるオンライン支払いサイトに関する無料チュートリアルを含む）
- 2000 枚　　9 ドル/枚（人気のあるオンライン支払いサイトに関する無料チュートリアルを含む）

盗難クレジットカードに「100 %の満足保証」、不満があればカード交換

アンダーグラウンドのハッカー市場における別の興味深い傾向は、ベンダーが顧客満足度向上を図るために、優れたカスタマサービスの提供に力を入れ出しており、中には高い顧客満足度の保証を掲げているベンダーも見受けられました。

図 1 では、ハッカーは販売中の盗難プレミアムクレジットカードについて「有効なカードの割合 100 %」を約束しています。例えば、100 枚のクレジットカードを購入した場合、それらのカードはすべて利用可能な状態です。ハッカーは「有効でないカードはすべて交換します」と明言しています。 さらに、同じベンダーは「クレジットカード保証」も提供しています。クレジットカードが 200ドルの支払いに通らない場合は、販売者が Try2Check（アンダーグラウンドで人気のあるクレジットカード検証アプリケーション）を使用してチェックし、利用不可のカードであれば交換されます。また、販売しているクレジットカードはすべてプレミアムカードであり、プラチナカード（クラシック/スタンダード）より低いカードの場合は、そのカードを交換することも保証しています。

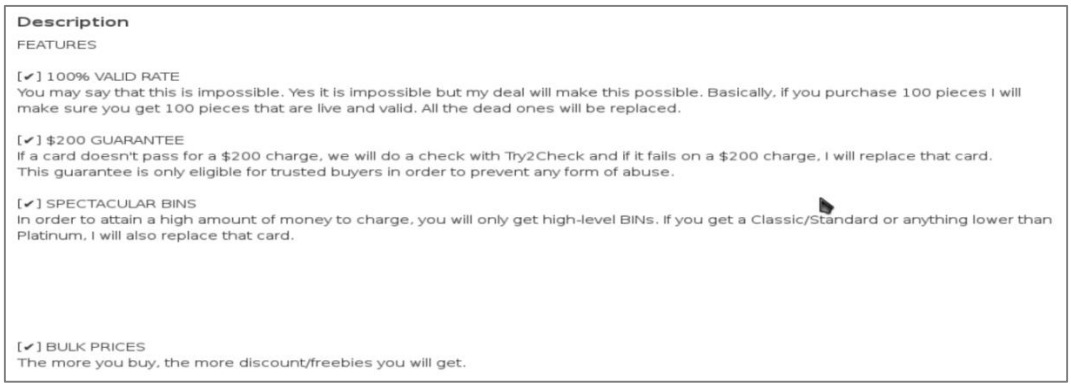


図 1: アンダーグラウンドの販売者の満足度保証の例

販売されているマルウェア

販売されているリモートアクセス型トロイの木馬（RAT: Remote Administration Tool）

リモートアクセス型トロイの木馬（RAT）は、ハッカーに標的とするコンピュータの管理制御権を与えるバックドアを含むマルウェアプログラムです。2014 年は RAT が 2013 年よりかなり安価になっていることを発見しました。現在、RAT は 20～50 ドルぐらいで、通常は次のものが含まれています。

- darkcomet
- blackshades
- cybergate
- predator pain
- Dark DDoser

2013 年の RAT の価格範囲は 50～250 ドルでした。価格が下がった背景には、ソースコードが漏れてから、アンダーグラウンドでは多くの RAT が無料で入手できるようになったからであると推測されます。
ハッカーは、簡単に購入できる、もしくは無料で使用でき、Crypter（マルウェアを暗号化し FUD にするか、ウイルス対策およびマルウェア対策プログラムでまったく検出できないようにするプログラム）で処理できる RAT を探しています。

販売されている Crypter

人気のある Crypter は 50～150 ドルほどで取引され、以下のものが含まれています。

- Aegis
- Sheikh Crypter
- xProtect

Crypter の価格は、マルウェアを暗号化して FUD できるかどうかで異なります。しかしながら、経験の長いハッカーの多くは独自の Crypter をコーディングする方法を知っているため、これらのツールを購入するハッカーはハッキングの経験が浅いか、そのようなスキル自体を持っていません。

販売されているエクスプロイトパック

エクスプロイトパックは、さまざまな悪意のあるプログラムが含まれたソフトウェアキットです。ハッキングされたウェブサイトや悪意のあるサイト上で実行されると、そのサイトにアクセスしたユーザのマシンで、ハッカーが多数のブラウザエクスプロイトを起動できるようになります。古いブラウザプラグインでこのようなサイトにアクセスした場合、何も表示されずにマルウェアがインストールされる可能性があります。本調査では、アンダーグラウンドのハッカーがよく話題にするエクスプロイトパックは、「Nuclear」と「Sweet Orange」の 2 つでした。

Nuclear エクスプロイトパックのリース料金

- 50 ドル/日
- 400 ドル/週
- 800 ドル/月

Sweet Orange エクスプロイトパックのリース料金

- 350 ドル/週
- 1,300 ドル/月

Nuclear と Sweet Orange は週あたりの価格は同程度ですが、Nuclear の 800 ドル/月のリース料金は、Sweet Orange の 1,300 ドル/月のリース料金よりかなり安くなっています。 Sweet Orange の方がコストはかかりますが、Nuclear より堅固なエクスプロイトキットであると考えられています。Sweet Orange には新型エクスプロイトが含まれており、より多くの組み込み機能を実装しています。

販売されている感染コンピュータ

2013 年に感染コンピュータ（ボット）の価格を調査した際には、特定の地域が指定されていないボットの大口購入価格だけを見つけました。これらランダムなボットはかなり安い価格で販売されていました。例えば、1,000 ボット/20 ドル、5,000 ボット/90 ドル、10,000 ボット/160 ドルほどで取引されていました。

しかし、2014 年の調査では、特定の国にあるボットの価格設定がより高値で販売されていることを発見しました。感染コンピュータへのアクセスの購入価格は国ごとに異なります。米国にある別々の 5,000 ボットの価格は 600～1,000 ドルですが、英国ベースの 5,000 ボットの価格は 400～500 ドル、米国のボットより 50～100 パーセント低い価格設定になっています。

米国の感染コンピュータの価格の方が高い理由として、米国のボットには英国のユーザがアクセスできない金融サイトへのアクセス権が含まれているためであると考えられています。例えば、ハッカーが Coinbase のビットコイン口座の盗難を目論んでいたとしても、Coinbase は米国在住の顧客とのみビジネスをしているため、ハッカーには米国にある感染コンピュータへのアクセス権が必要となります。 さらに、英国やヨーロッパでは Chip and PIN テクノロジが利用されていることが多いため、英国の感染ボットで見つかったクレジットカードの口座情報の方がセキュリティが高いと考えられます。

Chip and PIN テクノロジは EMV（Europay、MasterCard、Visa）とも呼ばれます。これを利用する場合は、実際の購入の場面で承認のために 4 桁の PIN 入力が必要になります。 また、チップに埋め込まれているすべてのデータと通信は暗号化技術によって保護されているため、Chip and PIN カードはハッキングがしにくい仕

様になっています。米国で利用されているクレジットカードの多くは、カードデータが従来の磁気ストライプにエンコードされており、比較的データの盗難が容易です。また、磁気ストライプのクレジットカードは、Chip and PIN カードより偽造がずっと容易です。磁気ストライプカードには PIN 入力が不要なため、窃盗犯は偽の署名を走り書きして立ち去ることができます。

米国（ユニークインストール）

- 1,000　140～190 ドル
- 5,000　600～1000 ドル
- 10,000　1100～2000 ドル

英国（ユニークインストール）

- 1,000　100～120 ドル
- 5,000　400～500 ドル
- 10,000　700～1100 ドル

アジア（ユニークインストール）

- 1,000　4～12 ドル
- 5,000/10,000　なし

販売されているオンライン銀行口座

盗難クレジットカードと同じように、オンライン銀行取引の資格情報も販売されています。 SecureWorks の企業ブランド監視チームは、70,000～150,000 ドルの「検証済み」残高があり、高価値と位置付けられているオンライン銀行口座のユーザ名とパスワードが、口座残高の 6 パーセントぐらいの価格で購入できることを発見しています。残高 70,000 ドルの口座の場合、購入金額は約 4,200 ドルです。

利用できるハッキングサービス: Web サイトへのハッキング、DDoS 攻撃、Doxing（個人情報の収集/公開）

Web サイトへのハッキング

Web サイトへのハッキングの現在の価格が 100～200 ドルの範囲にあることを確認しました。2013 年は 100～300 ドルでした。従来どおり価格はツールを販売するハッカーの評判によって変動します。評判のよいハッカーほど価格が高くなります。

分散型サービス拒否（DDoS）攻撃

ウェブサイトをオフラインで攻撃することをハッカーに依頼する際の価格は、2013 年の価格と同水準でした。ただし、DDoS 攻撃を 1 日または 1 週間続ける場合の価格は少し安めに設定されています。2014 年の価格の例を示します。

2014 年の DDoS 攻撃の価格	2013 年の DDoS 攻撃の価格
1 時間あたり 3～5 ドル	1 時間あたり 3～5 ドル
1 日あたり 60～90 ドル	1 日あたり 90～100 ドル
1 週間あたり 350～600 ドル	1 週間あたり 400～600 ドル

Doxing（個人情報の収集/公開）

販売されている Doxing サービスは 2013 年と比べて減少しています。Doxing を依頼すると、ハッカーはターゲットに関するすべての情報を収集します。これには、ソーシャルメディアサイトや公開情報サイトの検索 や、ソーシャルエンジニアリングを通じて被害者を操り、情報を盗むためのマルウェアに感染させることなどが含まれます。 Doxing サービスを販売しているハッカーの場合、25～100 ドルの価格を設定しています。

SecureWorks からのアドバイス

法人向け： 財務データ、個人を特定できる情報（PII）、および知的財産をセキュリティ侵害から保護する方法

- 犯罪活動から保護するために、組織にとっても個人にとっても、脅威に常に注意を払い、財務データ、PII、および知的財産の損失を防ぐ防護対策を実施することが重要です。 SecureWorks は、組織と個人の両方にとって重要な一連のセキュリティ設定手順をまとめました。

- セキュリティへの階層型アプローチをお勧めします。次のものを実装することを検討してください。
  1. ネットワークおよび Web アプリケーションを囲むファイアウォール
  2. 侵入防止システムまたは侵入検知システム（IPS/IDS）。 これらは出入りするトラフィックからサイバー攻撃を検査し、脅威を検出またはブロックします。
  3. ホスト侵入防止システム（IPS）
  4. エンドポイントおよびネットワーク向けの高度なマルウェア対策ソリューション
  5. 脆弱性スキャン
  6. 24 時間 365 日のログの監視、および Web アプリケーションとネットワークのスキャン
  7. 最新の脅威に関するセキュリティインテリジェンス（リアルタイムのヒューマンインテリジェンスで最新の脅威に取り組む従業員）
  8. 暗号化された E メール
  9. コンピュータのセキュリティ上の脅威、特にスピアフィッシングの試みを見抜く方法を従業員に教育することが重要です。 防護対策として重要なのは、送信元を知っている場合でも、E メールのリンクまたは添付ファイルを決してクリックしないように従業員を教育することです。従業員には、E メールのリンクまたは添付ファイルをクリックする前に送信元に確認させてください。 E メールと Web 閲覧は 2 つの主要感染経路です。

SecureWorks からのアドバイス

個人向け

以下のセキュリティ設定手順を検討してください。

1. コンピュータユーザは、オンラインバンキングと請求書の支払い専用のコンピュータを使用してください。 そのコンピュータまたは仮想デスクトップで E メールの送受信と Web の閲覧には使わないようにします。Web エクスプロイトと悪意のある E メールは、主要なマルウェア感染経路です。
2. 信頼できない送信元からの E メールのリンクまたは添付ファイルクリックするのを避けます。送信元がわかる場合でも、リンクまたは添付ファイルをクリックする前に、送信元がその E メールを送信したことを確認してください。
3. 定期的に銀行およびクレジットカードの明細をオンラインバンキングやクレジットカードの使用状況と照合して、口座の乗っ取りの可能性を示す異常な取引がないことを確認します。
4. ウイルス対策ソフトウェアが最新の状態で、新しいエクスプロイトから保護できることを確認します。また、ウイルス対策ソフトウェアのベンダーが最新のトロイの木馬を検出するための署名を持っていること、およびウイルス対策ソフトウェアの最新の保護機能をインストールしていることを確認します。
5. ウイルス対策製品の「試用版」を保護手段として使用しないでください。ウイルス対策製品の試用版は製品をテストするためには適していますが、自宅や仕事用の PC を保護するために試用版を使い続けてはいけません。 試用版では更新を受信できないため、試用版のリリース後に出てきたトロイの木馬やウイルスはその PC に完全にアクセスできます。
6. セキュリティ保護製品が実行されていることを確認します。ソフトウェアパッチの管理が重要です。パッチが入手可能になったらすぐに、アプリケーションやコンピュータのオペレーティングシステムの更新をインストールことが重要です。
7. ソフトウェア（特にダウンロードアクセラレータやスパイウェア削除ツールなど、話がうますぎるソフトウェア）のインストールに対して注意を怠らず、ユーザにダウンロード/実行/特権操作を求めるウェブサイトのポップアップには慎重に対処してください。 多くの場合、こういう無料ソフトウェアやポップアップにはマルウェアが埋め込まれています。
8. 新しい銀行またはクレジットの口座が申請されたときや、クレジットの残高が基準を超えたときに警告が発生されるように、3 in 1 のクレジット監視サービスに登録することを検討してください。

ハッカー市場で販売されている製品およびサービスの価格

ハッカー提供の資格情報およびサービス	2013 年の価格	2014 年の価格
Visa およびマスターカード（米国）	4 ドル	4 ドル
アメリカン・エキスプレス（米国）	7 ドル	6 ドル
ディスカバーカード（米国）	8 ドル	6 ドル
Visa およびマスターカード （英国、オーストラリア、カナダ）	7～8 ドル	8 ドル
アメリカン・エキスプレス （英国、オーストラリア、カナダ）	12～13 ドル	15 ドル（英国、オーストラリア）、 12 ドル（カナダ）
ディスカバーカード（オーストラリア、カナダ）	12 ドル	15 ドル（オーストラリア）、 10 ドル（カナダ）
Visa およびマスターカード（EU、アジア）	15 ドル	18～20 ドル
ディスカバーカード、アメリカン・エキスプレス （EU、アジア）	18 ドル	18～20 ドル
Track 1 および 2 データ付きの クレジットカード（米国）	12 ドル	12 ドル
Track 1 および 2 データ付きのクレジットカード （英国、オーストラリア、カナダ）	19～20 ドル	19～20 ドル
Track 1 および 2 データ付きのクレジットカード （EU、アジア）	28 ドル	28 ドル
Fullz（米国）	25 ドル	30 ドル
Fullz（英国、オーストラリア、カナダ、EU、アジア）	30～40 ドル	35～45 ドル
VBV（米国）	10 ドル	12 ドル
VBV（英国、オーストラリア、 カナダ、EU、アジア）	17～25 ドル	28 ドル
Track 1 および 2 データ付きの プレミアムマスターカード（全世界）	なし	35 ドル
Track 1 および 2 データ付きの プレミアム Visa カード（全世界）	不明	23 ドル
70,000～150,000 ドルの検証済み 残高のある高品質銀行口座	不明	口座残高の 6 %
リモートアクセス型トロイの木馬（RAT）	50～250 ドル	20～50 ドル
Crypter	不明	50～150 ドル
Sweet Orange エクスプロイトキットの リース料金	450 ドル/週、 1800 ドル/月	450 ドル/週、 1800 ドル/月
Nuclear エクスプロイトキットの リース料金	不明	50 ドル/日、400 ドル/週、 600 ドル/月

偽造パスポート（米国以外）	不明	200～500 ドル
新しい身分証明書、 および対応する公共料金請求書	不明	250 ドル、対応する公共料金請求書は 100 ドルの追加
偽造社会保障カード	不明	250～400 ドル
偽造運転免許証	不明	100～150 ドル
ハッキングのチュートリアル	不明	各 1 ドル～30 ドル/10 項目 （チュートリアルにより異なる）
Web サイトのハッキング、データの盗難	100～300 ドル	100～200 ドル
DDoS 攻撃	1 時間あたり 3～5 ドル	1 時間あたり 3～5 ドル
	1 日あたり 90～100 ドル	1 日あたり 60～90 ドル
	1 週間あたり、 400～600 ドル	1 週間あたり 350～600 ドル
Doxing（個人情報の収集/公開）	25～100 ドル	25～100 ドル
感染コンピュータ（米国）	不明	米国（ユニークインストール）
		1,000 - 140～190 ドル
		5,000 - 600～1000 ドル
		10,000 - 1100～2000 ドル
感染コンピュータ（英国）	不明	英国（ユニークインストール）
		1,000 - 100～120 ドル
		5,000 - 400～500 ドル
		10,000 - 700～1100 ドル
感染コンピュータ（アジア）	不明	アジア（ユニークインストール）
		1,000 - 4～12 ドル
		5,000/10,000 - なし

本レポートは、2014 年 12 月に SecureWorks が公表した内容の抄訳となります。

サービスの提供内容は国によって異なります。© 2014 Dell Inc. All rights reserved.

Dell および Dell ロゴ、SecureWorks、Counter Threat Unit（CTU）、および iSensor は、登録商標またはサービスマーク、もしくは米国およびその他の国における Dell Inc.の登録商標またはサービスマークです。言及された他の全ての製品とサービス、商標などはそれを保持する企業・団体に帰属します。本資料に記載されている内容は 2015 年 1 月時点のものであり、予告なく変更する場合があります。最新の仕様については、弊社営業またはホームページにてご確認ください。

- より詳細な内容は Web：www.secureworks.jp
- 弊社へのご連絡は E メール: Info-NorthAsia@secureworks.com