McAfee
An Intel Company

エグゼクティブ サマリー

デジタル通貨の問題点

デジタル通貨とサイバー犯罪における悪用について

Raj Samani — McAfee EMEA
François Paget、 Matthew Hart — McAfee® Labs

犯罪者が資金洗浄の手段としてデジタル通貨を利用していると言われていますが、最近の取締りや摘発を見ると、その傾向はさらに強くなっているようです。デジタル通貨サービスの Liberty Reserve は 60 億ドル以上の資金洗浄に関与し、業務停止処分を受けました。この金額は、国際的なマネーロンダリングの摘発としては過去最高の規模となっています。

犯罪者が利用している仮想通貨は Liberty Reserve だけではありません。このようなサービスはサイバー犯罪やネット上での破壊活動で頻繁に利用されています。マネーロンダリング以外にも、金融機関を狙う標的型攻撃やデジタル財布を狙うマルウェアなど、様々な危険が存在します。

Bitcoin などの仮想通貨では、マイニングという手法で通貨を発行することできます。当初は、発行者自身のコンピューターがマイニングに使用されていましたが、2011 年 6 月に Bitcoin を生成する JavaScript が登場し、サイトを閲覧したユーザーのコンピューターを利用して Bitcoins の発行ができるようになりました。この処理を訪問者に通知するサイトもありますが、不正なボットを構築し、ユーザーに知らせずに通貨を発行しているケースもあります。E-Sports Entertainment Association では約 14,000 台のコンピューターが Bitcoins のマイニングに利用されていました。

デジタル通貨の定義

ECB（欧州中央銀行）は、仮想通貨と電子マネーのスキームに大きな違いがあることを指摘しています。電子マネーは従来の通貨単位を利用し、管理されていますが、仮想通貨は規制を受けず、実在の通貨単位も使用していません。

Yankee Group は『Redefining Virtual Currency』（仮想通貨の再定義）の中で、仮想通貨市場は 2012 年に 475 億ドルに達し、5 年後の 2017 年に 554 億ドル規模になると予測しています。また、この著しい成長の要因として携帯端末の普及が考えられると分析しています。

顧客にとって仮想通貨には多くの利点があります。信頼性があり、即時性と匿名性を備えています。特定の通貨でプライバシーが問題になっていますが（特に Bitcoin）、市場ではむしろ匿名性が強化されています。この市場の反応は見逃せません。仮想通貨サービスに対する取締りが行われているにも関わらず、犯罪者は資金洗浄を行う新しいプラットフォームをすぐに見つけ出します。主要なプラットフォームを閉鎖するだけでは問題は解決しません。

図 1 から図 4 のように、違法サービスの多くは決済方法として仮想通貨だけを使用しています。仮想通貨のみを受け付けるサービスは今後も増加するでしょう。サイバー犯罪者や企業家にとって、仮想通貨の利用には明確なメリットがあります。

図 1. 盗まれたクレジットカード番号、PayPal や eBay などのオンライン アカウントの認証情報などの売買では、仮想通貨以外の決済方法が使用できない場合が多い。

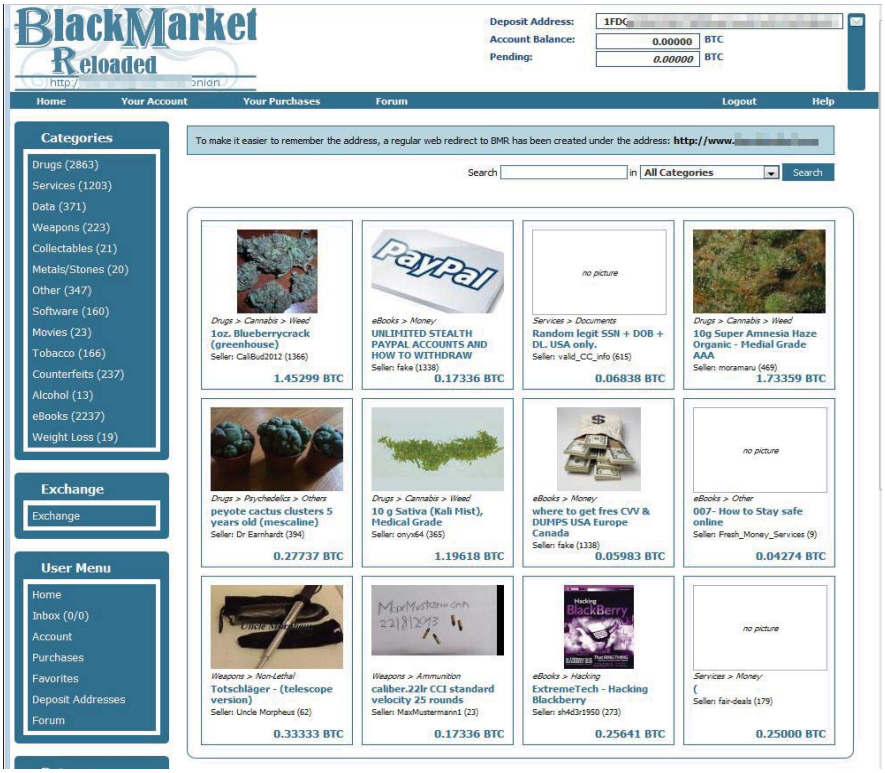

図 2. 匿名のオンライン マーケットでは、 違法製品の多くで決済方法として仮想通貨が使用されている。

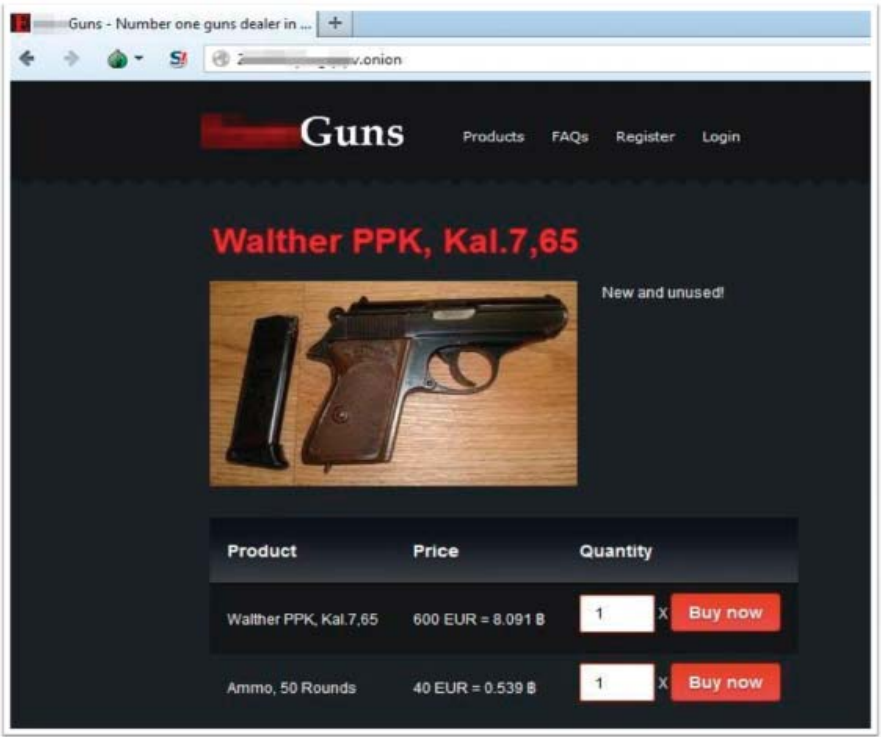

図 3. 銃などの規制対象品の販売でもよく利用されている。 仮想通貨の場合、 銃の販売を規制できないだけでなく、犯罪に使用された場合でも入手ルートの追跡が難しくなる。

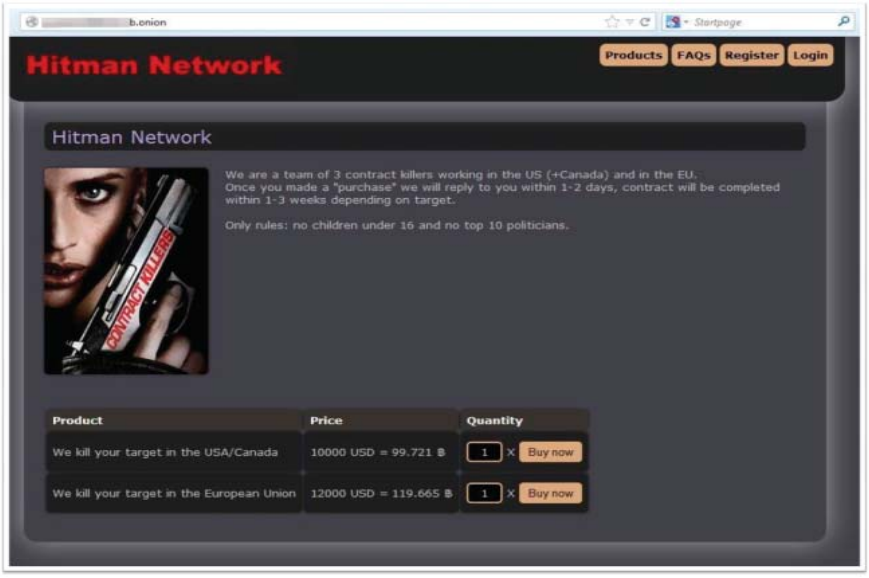

図 4. 16 歳未満の子供と最も重要な 10 人の政治家を除くターゲットの殺害を請け負う Hitman Network。 匿名での利用が可能。

デジタル通貨や電子マネーの最大のメリットは簡単に利用できる点です。 交換所で仮想通貨を取得する場合に登録が必要になる場合もありますが、 資金を用意すれば通貨を購入できる場合もあります。

Bitcoin は交換レートでも注目を集めている人気の仮想通貨です。2 月 28 日の交換レートは 1 BTC あたり 33 ドルでしたが、4 月 10 日には 266 ドルに急騰しました。 7 月は 100 ドル前後で推移し、 9 月 4 日には 144 ドルになりました。

当局の取締りを回避するため、 Bitcoin は暗号化と P2P 技術を使用しています。 捜査当局も認めているように、このアーキテクチャが不審人物の特定と取引記録の取得を困難にしています。

この分散化にも弱点はあります。 Bitcoin ネットワークにサービス拒否（DoS）攻撃が実行されたときに、開発チームはコアの設計部分の修正を余儀なくされています。 サイバー攻撃の標的になったのは Bitcoin のネットワークだけではありません。交換所も被害を受けています。

2011 年 6 月、 Bitcoin のメインの交換サイトである Mt.Gox がハッキングされました。 一連の詐欺行為で Bitcoin 経済は一週間も混乱し、 Bitcoin の交換レートは 17.50 ドルから大きく下落しました。

JavaScript による Bitcoin マイニング ツールが登場し、マイニングを行うボットが簡単に作成できるようになりました。 すべてのマイニングが不正なものとは限りませんが、 悪質な配布方法を利用することでマルウェアやボットが急増する可能性があります。 Bitcoin レートの最初の高等でも同じことが起きました。

McAfee Labs が最近行った Bitcoin ボットネットの調査では、 Bitcoin マイニング サービスと通信を行う別のボットネットも見つかりました。 攻撃者が提供した認証情報でオンラインのマイニング サービスに登録すると、これらのボットが指令サーバーの指示に従って処理を行い、 攻撃者に Bitcoins が発行される仕組みで、 2011 年 6 月には Allivain というハンドル名の Bitcoin ユーザーが 50 万ドルを盗まれています。

Bitcoin についてはプライバシーの問題も関心を集めています。 カリフォルニア大学サンディエゴ校とジョージ・メイソン大学の研究者が行った調査では、 透明性の確保を理由にすべての取引が Bitcoin のブロックチェーンに記録されるため匿名性の維持は難しいと報告しています。

結論

Liberty Reserve サービスの例を見ても分かるように、仮想通貨サービスを閉鎖してもサイバー犯罪者は新たな手段をすぐに見つけ出します。 犯罪者にとって有利な状況であっても、 捜査当局はこのようなサービスの運営者を特定し、 検挙するために、 海外の捜査機関や民間企業と協力して捜査を行っています。

仮想通貨がなくなることはないでしょう。 DoS 攻撃に対する脆弱性、マネーロンダリング、サイバー犯罪での利用など、問題はあるものの、 多くのユーザーが合法的な目的で利用しています。 このような市場で投資を始めるユーザーも少なくありません。 潜在的なリスクを解決しない限り、 被害も増加していきます。

このレポートの完全版については、http://www.mcafee.com/us/resources/white-papers/wp-digital-laundry.pdf（英語）をご覧ください。

マカフィー株式会社
www.mcafee.com/jp

東京本社　〒 150-0043 東京都渋谷区道玄坂 1- 12- 1
渋谷マークシティウェスト 20F
TEL 03-5428-1100（代）FAX 03-5428-1480
名古屋営業所　〒 460-0002 愛知県名古屋市中区丸の内 3-20-17
中外東京海上ビルディング 3F
TEL 052-954-9551（代）FAX 052-954-9552
西日本支店　〒 530- 0003 大阪府大阪市北区堂島 2-2-2
近鉄堂島ビル 18F
TEL 06-6344-1511（代）FAX 06-6344-1517
福岡営業所　〒 810- 0801 福岡県福岡市博多区中洲 5-3-8
アクア博多 5F
TEL 092-287-9674（代）

60589exs_digital-laundry_1013_fnl_ETMG