



G Data

Whitepaper 2010

アンダーグラウンド エコノミー Part2

G Dataセキュリティラボ

マークアウレル・エスター、ラルフ・ベントツミュラー、
& 瀧本往人(日本語版監修 + 序言)

(岸本真輔訳)



目次

日本語版への序文	3
概要	4
1 はじめに	5
2 裏経済の加担者を家宅搜索	5
3 商品・サービスへの影響	6
4 ペイセイフカードの事例	8
5 裏経済に関する今後の見通し	10
6 結論	11
付録 用語集	12

日本語版への序文

2010年5月25日、日本では「ロマンシング詐欺」と呼ばれる事件の首謀者2名が逮捕されました。これは、ファイル共有ネットワークを利用したウイルスによって金銭をだまし取ったという「詐欺」事件ですが、首謀者の1人がウイルス作者であり、ウイルス作者の逮捕としては、2008年1月に同じくファイル共有ソフトを利用する人々を狙った「原田ウイルス」の作者に次いで、2例目となりました。しかし、原田ウイルスが愉快犯であり、著作権侵害を理由とした逮捕であったのに対して、今回のロマンシング詐欺は、ウイルスを利用した金銭横領詐欺での摘発として、国内最初の事例となりました。

ロマンシング詐欺も、原田ウイルスと同様、ファイル共有ソフトのネットワークからダウンロードできるファイルにウイルスを仕込むという意味では、いわゆる「暴露系ウイルス」に分類されます。しかし今回の、犯行に使用された Kenzero (または Kenzo) という名称を付したウイルスは、違法にダウンロードしたファイル (アダルトゲームやオフィスソフトなど) をインストールする際に、個人情報を入力させる架空の機関 (国際著作権機構 (ICO)) のウェブページへ誘導するだけでなく、獲得した個人情報をもとにユーザーに金銭を要求し実際に横領しました。

このような、ウイルスを使用した犯罪は断じて許されるべきものではありません。しかし同時に、違法と知りながらファイル共有ネットワークなどから映像や音楽、ソフトなどをダウンロードしてはならないとする改正著作権法が1月より施行されているなか、金銭被害にあったユーザーにおいても著作権物の不正入手においては加害者であるという点は、今後、考えてゆかねばならないでしょう。

話は変わりますが、ドイツにおいては、昨年秋に、ネット犯罪のシンジケートを構成している一部の組織が集中して警察当局によって一斉捜索されました。詳しいことはホワイトペーパー本文をご覧くださいなのですが、ドイツの犯罪組織の手口は、違法に相当額の金銭を入手できる犯罪システムとしては、すでにかかなりの完成度に達していることがわかります。

それに対して、日本で起こったロマンシング詐欺事件は、それほど大掛かりものではなく、小規模であり、また、とても組織的な犯罪とは言えません。そもそもこのロマンシング詐欺事件は、すでに逮捕の2ヶ月ほど前より、ネット掲示板などにて被害報告や加害者の弾劾などが行われており、マスコミや警察当局も、それほど苦もなく本件の状況を詳細に把握できたと思われれます。

その意味では、日本で起こった事件は、あくまでも、小さなコミュニティにおける小さな犯罪 (= ムラのウイルス犯罪) という位置づけになるのではないのでしょうか。対してドイツの事例は、国際規模での大掛かりな犯罪 (= グローバルなウイルス犯罪) とみなすことができます。

私たち日本に住む者としては、両者の事件から、一方では、将来的に、日本もドイツのようなグローバルなウイルス犯罪が増加する危険性をはらみつつつあることを理解しながら、他方では、依然として、ムラのウイルス犯罪もまた、引き続き、頻発するおそれがあると考え、この、両面における対策を怠らないようにすべきでしょう。そのためにも、本ホワイトペーパーを活用していただければと思います。

G Data Software
瀧本 往人
(2010年6月3日)

概要

ネット裏市場への警察の対応

- ・昨年末にドイツとオーストリアでサイバー犯罪者の家宅捜索が実施されました。約 50 軒の住居が対象となり、4 名が逮捕されました。

- ・警察の報告によると、この家宅捜索では、裏経済フォーラム「1337 Crew」(発音: リートクルー。1337 を leet と読む)による 10 万台以上ものボットに感染した PC が押収された模様。

- ・摘発後は、多数の掲示板やショップがオフラインの状態となりました。これは、警察の捜査から身を隠すため、または、裏経済関連の逮捕者が他にも出て、運営がままならない状態のためだと考えられています。オンライン犯罪者の多くが、今回の捜査をきっかけに、業界から一時的に(もしくは永久に)身を引いた可能性があります。

- ・しかし、リートクルーの摘発の効果は、当初期待されたほどの変化をもたらすことができませんでした。闇市場は消えることなく引き続き存在し、その市場の構造にもそれほど変化は与えませんでした。実際のところ、リートクルーの後釜につこうとするフォーラムがすでに存在しています。

ペイメントサービス業者への攻撃

- ・闇市場で好まれて利用されていた支払いサービス業者は「ペイセーフカード」でした。しかし、2010 年 2 月に行われたシステムの変更により、流れていた大量の資金が凍結させられることになりました。そこで、サイバー犯罪者たちは、ペイセーフカードに対し、DDoS 攻撃を決起しました。その結果、システムの変更は、翌日修正されました。

取引が行われるフォーラムでの変化

- ・販売システムの変化として、以前は独占的な販売者だけが費用を払うという体制がとられていましたが、詐欺被害を避けるため、全てのショップ運営者から支払いを求める体制へ変更となりました。

- ・犯罪フォーラムの運営者は学習を重ね、今は、匿名性、安全性、評判に重点を置いています。その 1 つには、フォーラムへの入会金導入などがあります。また、フォーラム内部でのそれぞれの会員の評価や評判も、重要性が高くなってきています。

売買価格の実態

- ・昨年末の調査以来、売買価格自体にはほぼ変化がみられず、価格は業者、ディスカウント、交渉、または需要と供給のバランスによって変わってきます。

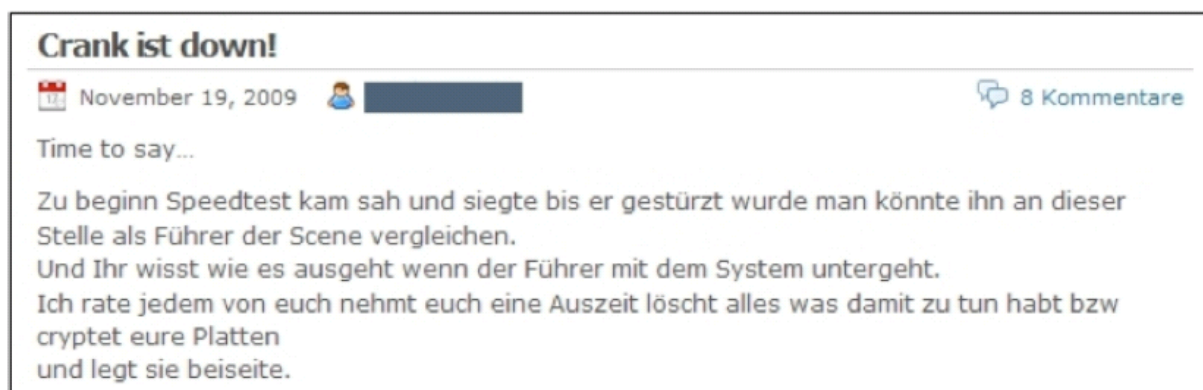
1. はじめに

2009年9月の裏経済に関するホワイトペーパーの発表後、裏経済に変化が見られました。今回は、2009年11月の警察の家宅捜索に焦点をあてながら、裏経済における最近のインシデントについて説明します。

2. 裏経済の加担者を家宅捜索

2009年11月、サイバー犯罪者たちの大規模な家宅捜索が行われたことにより、その後サイバー犯罪者の環境に変化が見られました。ドイツとオーストリアの警察から200人以上の警察官が出動し、約50軒を対象とした大規模な家宅捜査が行われ、4名が逮捕されました。対象となったのは、ドイツ最大級といわれる地下フォーラムであるリートクルーのプラットフォームでした。

コンピュータ犯罪者の間では、フォーラムの首謀者（別称「Speedtest」以下「スピードテスト」と記載）が警察側に屈し、大量の関連資料を警察側に提示したという憶測が流れ、ネット犯罪者たちは、スピードテストを裏切り者と非難しました。今のところ、当局側へどのような資料が渡ったのかは公表されていないので、その辺りに関する事実はわかりませんが、スピードテストがこの家宅捜索が行われたその日のうちに釈放されたのは、非常に興味深い事実でした。



スクリーンショット1: 地下ブログにて、11月の家宅捜索に関する投稿

警察の発表によると、リートクルーは10万台の感染したゾンビPCを支配下に置くボットネットを操っていました。

また、捜査対象となったのは、リートクルーだけではありませんでした。裏経済で暗躍するその他多くの掲示板、ブログ、ショップもその活動を停止しました。このうちの一部は、検挙を免れるための対策として、自主的に停止したようですが、関係者が逮捕された掲示板

もあったようです。また、警察による掲示板へのアクセスを恐れた一部のものが、その掲示板に対して DDoS 攻撃を行うといったこともありました。



スクリーンショット2: 裏経済で名が知れ渡っているショップもサービス停止に追い込まれました(画像にはサービス再開の記述がありますが、実際は行われていません)

3. 商品・サービスへの影響

有名なコミュニティのサービス停止は、一定の作用をもたらしたものの、裏経済の市場に決定的な打撃を与えることはできませんでした。警察の捜査後、供給価格やモノの供給自体に大きな変化はみられず、変動幅も通常の範囲内で動いています。これは裏経済の大部分が国外に所在していることに起因しています。ドイツやオーストリアにとっては大規模である家宅搜索も、業界全体からみると、まさに焼け石に水であった、と考えられています。

名称	価格 (ユーロ)
フィッシングされたバックステーション(無人の小包発送受取所)アカウント	
ポスト番号+ Pin + PW	30
ポスト番号+ Pin + PW + メール	50
ポスト番号+ Pin + PW + SMS 送信設定オフ	40

PayPal Accounts	
PayPal + 銀行情報、Email 付	4
PayPal + クレジットカード情報 + クレジット 付	20
PayPal + クレジットカード情報、Email 付	8

名称	価格 (ユーロ)
Steam アカウント	
エイリアン VS プレデター(完全版)	10
コール オブ デューティ: モダンウォーフェア 2(完全版)	15
カウンターストライク 1.6	7
カウンターストライク(ソース)	10
レフト 4 デッド 1	10
レフト 4 デッド 2(完全版)	15
メトロ 2033(完全版)	12
オレンジボックス	10

PayPal + eBay、メール付	10	サブリーム・コマンダー2	12
携帯電話		ゲーム時間&ポイント	
Vodafone SIM カード 25 個(発送先: Packstation)	25	1,000 Wii ポイント	5
Vodafone SIM カード 6 個(発送先: Packstation)	10	50 欧州版 PS ネットワークカード	18
Vodafone SIM カード 8 個(発送先: Packstation)	10	800 Xbox ポイント	5
薬物		NC ソフト 60 日ゲーム分	10
バイアグラ 4 錠	20	WoW60 日ゲーム分	10
		Xbox ライブ 12 ヶ月ゴールド	15
		Xboxraibu ポイントカード 4,200	18

表1: 裏経済ショップの取引品および同最新価格

裏経済のネットワークでは、今も尚、犯罪に悪用される様々な違法な取引物（クレジットカード情報から偽造書類、数十万円するスキミング機材まで）を犯罪者は手に入れることができます。



写真1: 携帯カードリーダー MSR500M (220-270US ドル) 写真2: 改変セット GSM Skimmer (2,000-6,000US ユーロ)

また、裏経済で取引される機材の質もあがり、プロレベルの機材や材料（デザインもアレンジできるクレジットカード材料など）の取引数が増加傾向にあります。価格は、カード一式につき 50～150 ユーロで、通常は 10 個以上からの注文が可能です。このカード材料に盗難されたクレジットカード情報をコピーし、小売店での犯罪（Instore-Carding）で導入されます。Instore-Carding のメリットは、品をその場で手にすることができる点で、郵送などで必要な中継点を経由する手間を省くことができます。しかしながら、個人的に店を訪れてカードを使用しなければならぬため、相応のリスクが発生します。

カード改変装置	最低価格	最高価格	
クレジットカード材料	45US ドル	150US ドル	ホログラム付きなど仕様により価格が大きく異なる。10 枚から購入可能
カードプリンター	450 ユーロ	3,500 ユーロ	カード材料からカードを作り出すためのカードプリンター
カードリーダー	250 ユーロ	900 ユーロ	クレジットカードや銀行のキャッシュカードを読み取るため

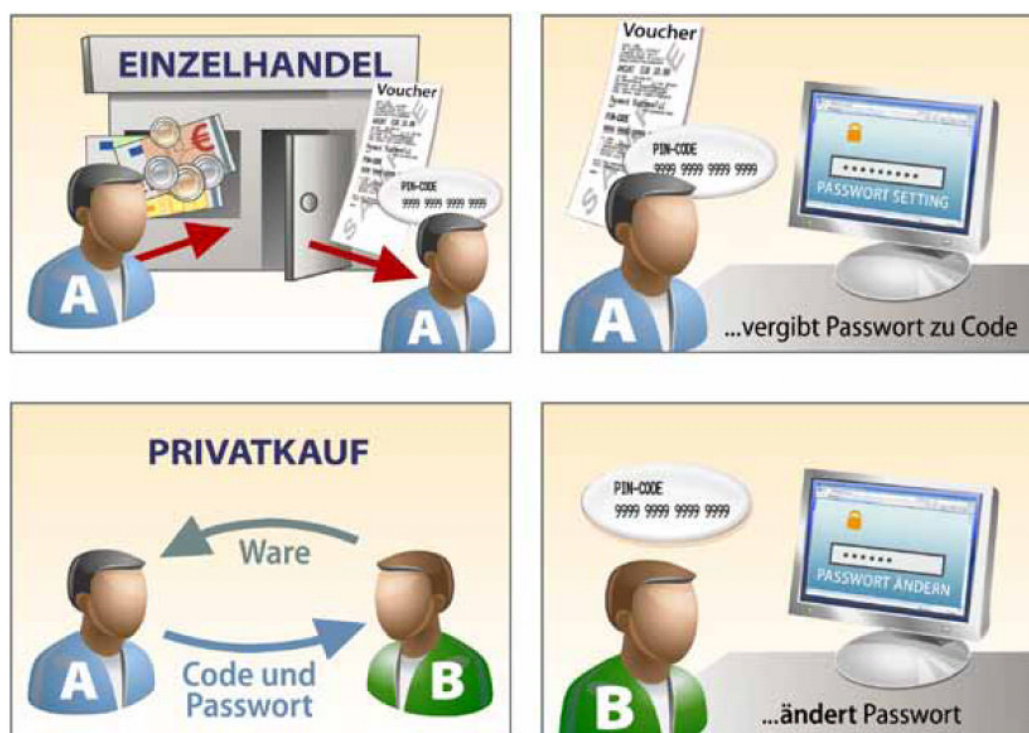
			の携帯カードリーダー
スキミングセット	1,500USドル	10,000USドル	様々な仕様あり。無線スキマーやビデオスキマーなど。

表2： 裏経済のショップでのカーディング製品の価格レンジ

4. ペイセーフカードの事例

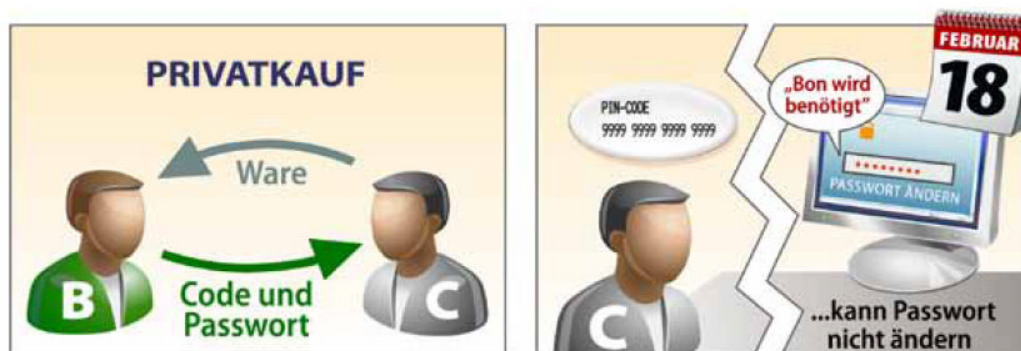
送金サービス業者のペイセーフカードがパスワード使用に関するシステム変更を発表した際、裏経済の業界中で悲鳴が上がりました。

通常、ペイセーフカードの利用者は、支払いもしくは第三者へペイセーフカード内の金額を引き渡すために、保護用の16桁からなるパスワードをかけます。



事例1: AさんはBさんからモノを買いました。Aさんは、支払い時にネットバンキングやクレジットカードで取引したくないので、モノの代金分のペイセーフカードを購入し、そのペイセーフカードのPINコードとパスワードをBさんに渡します。商品分のペイセーフカードを受け取ったBさんは、ウェブ上で受け取ったペイセーフカードのパスワードを変更することにより取引金額を受領したことになり、取引完了となります。また、Bさんは一度受け取った仮想マネーを更なる第三者との取引の支払いに利用することができ、仮想マネーの転用回数には制限がありませんでした。

2010年2月18日にペイセーフカードは、新しいPINコードにパスワード追加またはパスワード変更の無効化し、新規パスワードの作成や古いパスワードの変更するには、ペイセーフカード購入時のレシートの提示が必要とする、システム変更の発表を行いました。



事例2: そうこうするうちに、BさんがAさんから受け取ったペイセーフカードのお金を、BさんからCさんに渡ったとした場合、Cさんがペイセーフカードのレシートを手に入れるのは非常に困難で、Cさんのペイセーフカードは凍結状態となってしまいます。

この変更は、ペイセーフカードサービスを利用する全ユーザーが対象でしたが、ペイセーフカードの利用が好まれている裏経済では、大量のお金とその価値を失うことになったのです。結果として、闇ブログや掲示板の関係者は、ペイセーフカードのウェブサイトである「www.paysafecard.com」に対して、DDoS 攻撃を仕掛けることとなりました。

PaySafeCard.com unter DDoS

by [redacted]

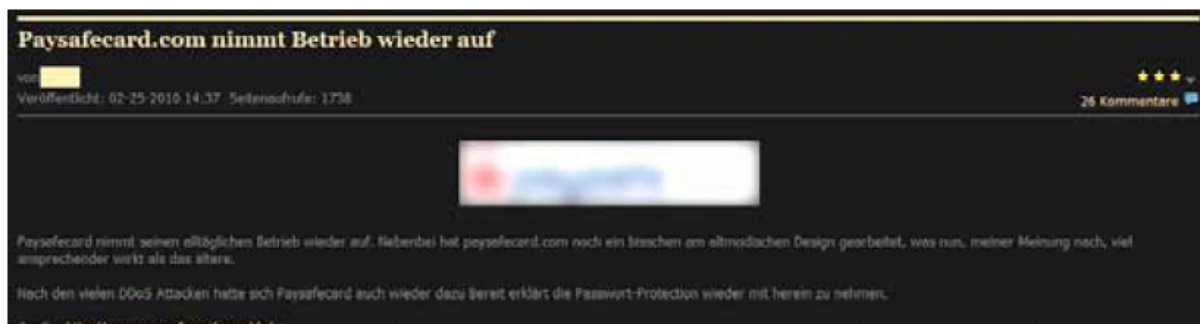
Published on 02-18-2010 17:14 111 Comments

Nach dem PaySafeCard.com PSC's mit Passwort fast wertlos machten, da man nun den Bon brauchte um das PW zu ändern bzw eine PSC mit PW zu benutzen, wollte sich das einige Mitglieder dieser Scene nicht gefallen lassen und schlagen nun zurück. Zum DDoS auf <http://www.paysafecard.com/> wird aufgerufen, egal wie groß das Botnet ist.

スクリーンショット3: ペイセーフカードに対する DDoS 攻撃の蜂起

ペイセーフカードのサイトは、公式的にはメンテナンスとのサイト上で表示していましたが、長い間ダウンの状態が続き、実際のところ攻撃によるダウンなのかメンテナンスなのかはわかっていません。

しかし、DDoS 攻撃蜂起が起こった、たった1日後の2010年2月19日、ペイセーフカードは、「2010年2月22日までに行われたパスワード設定や変更はレシート送付なしで可能」とのパスワード管理に関するルールを修正しました。ハッカー攻撃に関する公式発表はありませんでしたが、裏経済ではDDoS 攻撃に屈したペイセーフカードが新たな条件を提示したとされています。

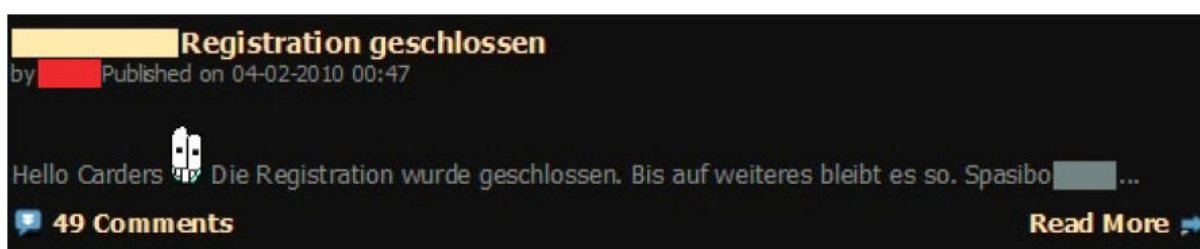


スクリーンショット 4: ペイセーフカードに関する地下フォーラムのメンバーによるコメント

5. 裏経済に関する今後の見通し

摘発後まもなくリートクルーの後継を謳う新たな十数個の掲示板が登場しました。このうちの数個の掲示板はすでにオフライン（サービス停止）状態になっていますが、その原因はハッカー攻撃によるものです。

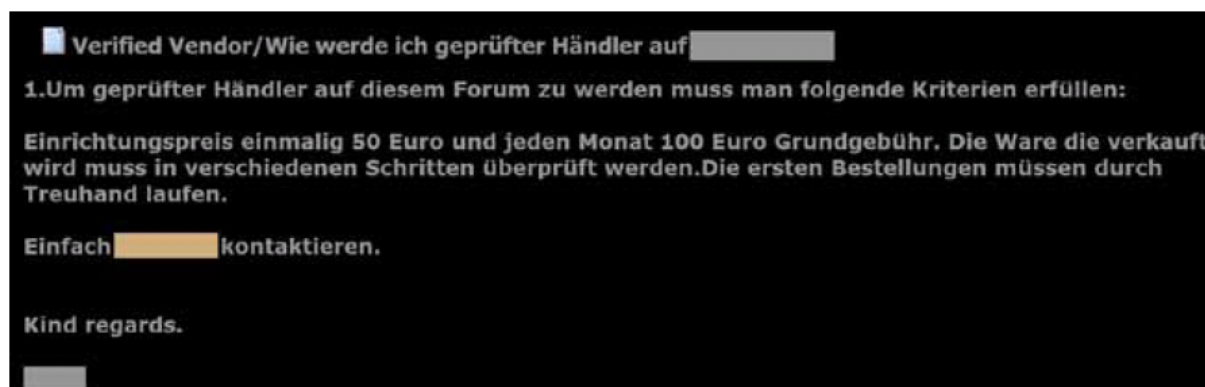
裏経済コミュニティのいくつかは、自身を保護するために、一時的に興味深い方法をとっていました。その1つには、参加費の導入があります。ペイセーフカードのような仮想通貨を10ユーロ分支払って初めて、サービスを利用したり、フォーラムで活動できるようになります。しかし、この支払登録制度は、反対意見が多かったのか、今は廃止されています。現在は、登録は必要なしで裏フォーラムの利用ができるようになっていますが、なぜこのようになったのかは理由が明らかにされていません。



スクリーンショット 5: 2010年4月上旬から登録が不可能に

物品の販売ルールにも変化がありました。この掲示板では登録制（前払制）で、それは「パテント」と呼ばれていました。

数百ユーロのパテントを支払うことにより、売り手は、掲示板で独占的にクレジットカードを販売する権利を得ることができるのです。より安価にショップライセンスを購入することも可能なのですが、それは独占的に販売する権利を得られるものではありません。今現在は、スタンダードな販売店ライセンスのみが存在しているだけで、パテントライセンスは廃止されています。それぞれの販売者が金額を支払って、販売権を得ています。このシステムで、掲示板には資金が流れ込み、同時に内部の詐欺師からも保護できると考えられています。



スクリーンショット 6: ショップ設立における掲示板の規約

もちろん新しいショップもある一方で、古いショップも営業が続けられています。両者とも掲示板、もしくはその周辺と深く結びついています。

また傾向として、ユーザー評価システムがより重視されるようになってきています。掲示板ではランキング表示がなされ、それぞれのユーザーの信用度ステータスを確認できるようになっています。このユーザー評価システム自体は新しいものではありませんが、重視されるようになってきたのは最近になってからです。

全体的に言えることは、裏経済業界全体が、以前より自身の安全性や匿名性を担保を心がけるようになってきました。また、リートクルーの摘発を契機に、裏経済に携わる者の多くが、「裏経済のメカニズムは自分たちが考えていたほど安全ではなかった」とその認識を変えています。これにより、一時的ではあるかもしれませんが、今まで裏経済を生業としていたものが、警察の捜査から逃れるために、足を洗ったと考えられます。

6. 結論

今回の調査により、裏経済関係者の関連当局の捜査に対して敏感になり、ショップや掲示板の事前遮断や裏経済コミュニティ内でのルールなどの様々な対策がなされるようになってきたことがわかりました。

また、犯罪者の多くが、一時的に身を隠すために潜伏したり、他のフォーラムに移っています。裏経済関係者には、将来的な警察の新たな捜査に対する恐怖を少なからずは残したように見受けられます。

裏経済関係者の報復と考えられているペイセーフカードの事件にみられるように、自身に損害を与えるものに対しては、競合やライバルなどの垣根を超え、業界全体で一致団結し、徹底抗戦するのも、一つの特徴と言えるでしょう。

裏経済コミュニティの保護メカニズムが上がり、より保護レベルの高いプラットフォームに集中することで、今後は、何が裏経済で起こっているかを外部から把握することがより困難になると考えられます。

付録 用語集

リートクルー (1337 Crew) 「1337 Crew」は掲示板の名称。この名称には、IT業界で使われるリートスピーク(暗号的なスラング)が使われています。リートスピークは、アルファベットを数字で見立てるのが特長です。例えば、リートスピーク(leetspeak)をリートスピーク形式で記載すると、「13375P34K」となります。またこのLeet(=1337)は、英語のEliteから来ています。

ボットネット (Botnet) ネット犯罪者が複数の外部のPCを操って攻撃を行う、そのネットワークのこと。操られるPCはボットもしくはゾンビPCと呼ばれる。DoS攻撃を仕掛けたり、スパムメールを大量配布したり、さまざまな用途で使用されます。

ボット (Bot) ロボットの略。不正に遠隔操作されたマシンのこと。

DoS 攻撃 (Denial of Service Attack) サービスを妨害する攻撃です。狙われたコンピュータ(たいていはウェブサーバーに、大量のデータや不正パケットが送りつけられ、サービスが不能化します。

DDoS 攻撃 (Distributed Denial of Service Attack) DoS 攻撃と同じ原理に基づいていますが、分散して攻撃を行う点が特徴です。指令者が第三者のマシンを「踏み台」(=ゾンビPC)にして攻撃を行うので、大規模な攻撃ができ、かつ、指令者が特定されにくくなります。

ペイセーフカード (Paysafecard) プリペイド形式のネット決済を提供する企業。クレジットカード、銀行振り込み、現金支払いの代替ソリューションとして、2000年からサービスが開始され、クレジットカードを所持していない人やクレジットカードを好んで利用しない人、匿名性を維持したい人々(闇経済に関わる人物も含む)に好んで使われ、現在、ヨーロッパをはじめ、世界中で利用されるようになってきました。ドイツでは、10ユーロから100ユーロのペイセーフカードが販売されており、ガソリンスタンド・ドラッグストア・キオスク・自動販売機から手軽に購入できます。

スキミング (Skimming) カード情報を抜き出して複製のカードを作る犯罪のこと。

スパム (Spam) 迷惑メールのことです。スパムという言葉はよく知られているように、モンティ・パイソンのコントに由来します(レストランのメニューがみなスパムの組み合わせから成り立っており、客と店員が注文するたびにスパム!を連呼するものです。YouTubeで見ることができます)。いまやスパムは多様な使われ方をされていて、広い意味ではすべての望まれないメールを指すこともあれば、狭義には、未承諾宣伝メール、ワーム添付のメール、デマメール、フィッシングメールを含む場合もあります。

ゾンビPC (ZombiePC) バックドアを通じて遠隔操作できるPCのこと。ゾンビ関連の映画がまさしくそうであったように、ゾンビPCは見えないマスター(ボットマスター、ハーダー)に従い、しばしば犯罪の片棒をかつぎます。通常多くのゾンビがボットネットに統合されています。

発行

28th May 2010

G Data Software株式会社