proofpoint

Proofpoint Threat Report

July 2012

本レポートは、Proofpoint が注目し、お客様および一般企業に対して注意を喚起したいと考えている脅威に関する情報、詳細、トレンドなどをまとめたものです。

Threat News（ニュース）

Grum ボットネットの解体

7 月 18 日、大規模ボットネットの Grum が解体され、全世界のスパムトラフィックが一時的に落ち込みました。企業及び非営利の研究者チームがコマンド＆コントロールセンター（CnC）を解体したのです。ウクライナの ISP である SteepHost が 23 日に短時間 CnC を復活させてしまいましたが、今はまた解体されています。Grum は世界で 3 番目に大きいボットネットと考えられていましたが、解体の影響は限定的でした。スパムトラフィックは 18 日には大きく落ち込みましたが、ウクライナのトラフィックが復活したため、一時急増しました。しかし、ウクライナの CnC が再度解体され、Grum ボットネットが永久に沈黙しても、トラフィックは減りませんでした。2011 年 3 月に Rustock ボットネットが解体されたときとは違い、Grum の解体はスパム量に恒常的な変化を与えることは無かったのです。

標的型攻撃の経済的影響

報道では有名企業へのスピアフィッシングや標的型攻撃のニュースが多く取り上げられますが、その陰で、中小の企業への攻撃が増加しています。Brian Krebs のレポート（http://krebsonsecurity.com/2012/08/uptick-in-cyber-attacks-on-small-businesses/）には、これらの攻撃によって経済的な被害を受けた事例をいくつか紹介しています。その中に、ジョージア州南部の燃料販売店で、経営者がメール中のイメージをクリックしてしまったがために 167 万ドルを送金され

れそうになった事例が紹介されています。イメージ中のリンクは BlackHole Exploit Kit に誘導されており、Zeus Trojan が PC にインストールされてコントロールを奪われてしまいます。

こういった、中小の企業を狙った攻撃は、その地域の小さな銀行の「緩い」セキュリティを狙うところが特徴です。多くの場合、そういった企業アカウントへのアクセスにはユーザーID とパスワードの単純な組み合わせで良いからです。しかし、二要素認証を導入すれば良いというものでもありません。「High Roller」の攻撃モデルがほとんどの二要素認証を自動化された手法で突破したことを思い出してください。その結果、EU のサイバーセキュリティ部局である ENISA は、金融機関は全ての顧客のシステムが侵害されていると仮定して対策をとるよう発表しました。(http://www.enisa.europa.eu/media/press-releases/eu-cyber-security-agency-enisa-201chigh-roller201d-online-bank-robberies-reveal-security-gaps) 通信路を保護するだけでは十分では無くなっているのです。金融機関は、トランザクションの相手が侵害されたシステムかもしれない、という前提で電子取引モデルを構築する必要があります。

サイバー攻撃に対する米国の準備状況

米国サイバー軍司令官の Keith Alexander 陸軍大将は、重要なネットワークインフラへのサイバー攻撃への備えという意味では、アメリカは 10 段階のうちで 3 番目にあるとコメントしました。(http://www.af.mil/news/story.asp?id=123311659) こういった攻撃はネットワークインフラの崩壊 (時には物理的な) を伴いうるもので、重要な情報の伝達に深刻な影響を与える DDoS 攻撃も同時に起こりえます。この問題は政府機関だけで無く、民間企業にも同様の大きな影響を与えます。大将のコメントは衝撃的ですが、驚きではありません。その代わりに私たちは、政府・民間企業・個人が協力して、この何時起きてもおかしくない攻撃に備えて、真にセキュアなポリシーや防御策を考え出さなければならないのです。

盗難パスワード

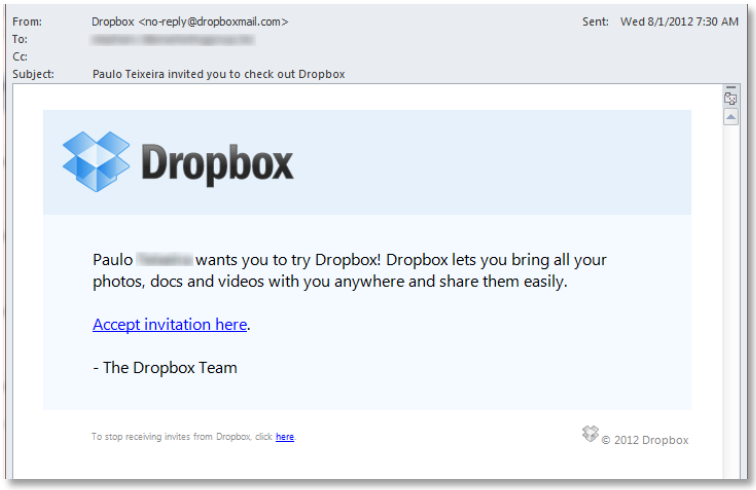
Yahoo Voices、Formspring、Nvidia および Phandroid の情報漏洩事件では、盗まれたパスワードがネット上で公開されたという発表が 7 月にありました。その中で Yahoo Voices の事件だけが平文のパスワードが公開されました。また、Dropbox が利用者の E メールアドレスが流出したと発表しました。同社の従業員が他の Web サイトで使っていたパスワードが盗まれ、そのパスワードがその従業員の Dropbox アカウントにも使われていたために起きた事件です。(http://blog.dropbox.com/index.php/security-update-new-features/) この E メールアドレスのリストはその後スパムのターゲットにされました。

どちらのケースも、複数のサイトで同じパスワードを使うことのリスクを浮き彫りにしました。盗まれたパスワードが公開されることは、企業のセキュリティホールの存在を白日の下にさらし、企業イメージを損ないますが、同時に様々に悪用される恐れがあります。個人のメールアカウントやその他の Web サービス(Dropbox のような)にアクセスし、データを盗もうとするか、多くの場合にはスパムや標的型攻撃に使われます。さらに、これらのログイン情報は VPN を通じて企業ネットワークに入り込むことにも使われ、データを盗み出したり、永続的な侵入口となるようなマルウェアを埋め込んだりします。

Threat Models（手法）

Dropbox

このメッセージは、Dropbox（上記を参照）のユーザー向けに送られたスパムの例です。これまでに他の Web サービスの例でも紹介してきたように、このメールもまた、正規の発信元から送られた有効なメールです。メッセージの内容は完全に正常です。こういったメッセージをブロックする為には、個々の Dropbox URL のパス全体をブロックするしかありません。


From: Dropbox <no-reply@dropboxmail.com> Sent: Wed 8/1/2012 7:30 AM
To:
Cc:
Subject: Paulo Teixeira invited you to check out Dropbox

Dropbox

Paulo wants you to try Dropbox! Dropbox lets you bring all your photos, docs and videos with you anywhere and share them easily.

Accept invitation here.

- The Dropbox Team

To stop receiving invites from Dropbox, click here.

© 2012 Dropbox

Airline Phish

航空会社は相変わらずフィッシングやスパムによく利用されます。この例では、Delta Airline になりすましており、全てのリンクは BlackHole Exploit Kit を含む単一のサイトを指し示しています。月末近くには、US Air を騙るメールが増加しました。

From: Tom Crosby <zkbvrrwrymkhr@hideakifan.com> Sent: Fri 7/6/2012 5:51 AM
To:
Cc:
Subject: Your Receipt and Itinerary

Thank you for choosing Delta. We encourage you to review this information before your trip. If you need to contact Delta or check on your flight information, go to delta.com, call 800-221-1212 or call the number on the back of your SkyMiles© card.

Now, managing your travel plans just got easier. You can exchange, reissue and refund electronic tickets at delta.com. Take control and make changes to your itineraries at delta.com/itineraries.

Speed through the airport. Check-in online for your flight.

Flight Information

DELTA CONFIRMATION #: A5XL99
TICKET #: 66274755238785

Day	Date	Flight	Status	Bkng Class	City	Time	Meals/ Other	Seat/ Cabin
Sun	8 JUL	DELTA 116	OK	U	LV NYC-KENNEDY	515P	F	45A
					AR SAN FRANCISCO	916P		COACH
Mon	9 JUL	DELTA 1837	OK	K	LV SAN FRANCISCO	1230P	V	32A
					AR NYC-KENNEDY	702A#		COACH

Baggage and check-in requirements vary by airport and airline, so please check with the operating carrier on your ticket.

Please review Delta's check-in Requirements and baggage guidelines for details.

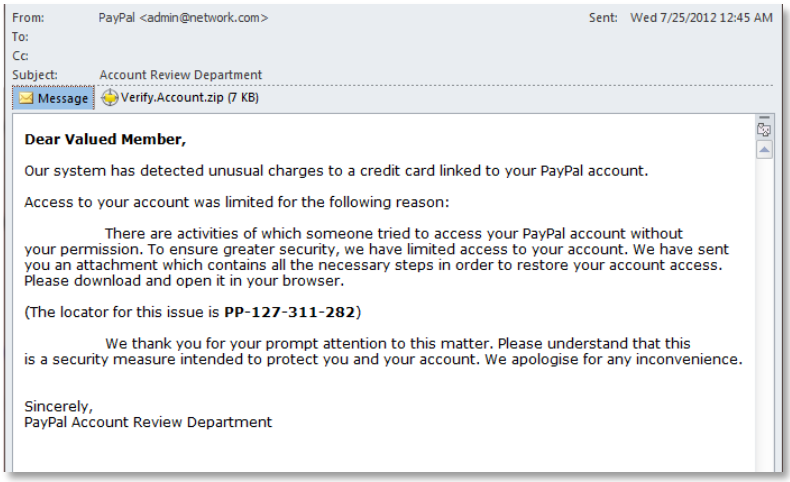
You must be checked in and at the gate at least 15 minutes before your scheduled departure time for travel inside the United States.

You must be checked in and at the gate at least 45 minutes before your scheduled departure time for international travel.

For tips on flying safely with laptops, cell phones, and other battery-powered devices, please visit http://SafeTravel.dot.gov.

PayPal

この PayPal を騙るメールに添付されている zip ファイルには HTML ファイルが含まれています。メール本体には夥しい文法上の間違いが見られますが、HTML ファイルは本物の PayPal の Web ページから作られています。ユーザーは社会保障番号やクレジットカード・デビッドカードの番号など、様々な個人情報を入力するよう促され、「送信」ボタンをクリックすると、データはロシアの Web ページへ送られ、即座に正規の PayPal サイトにリダイレクトされます。犯罪者はデータを入手し、ユーザーはそれに気づきません。



From: PayPal <admin@network.com> Sent: Wed 7/25/2012 12:45 AM
To:
Cc:
Subject: Account Review Department
Message Verify.Account.zip (7 KB)

Dear Valued Member,

Our system has detected unusual charges to a credit card linked to your PayPal account.

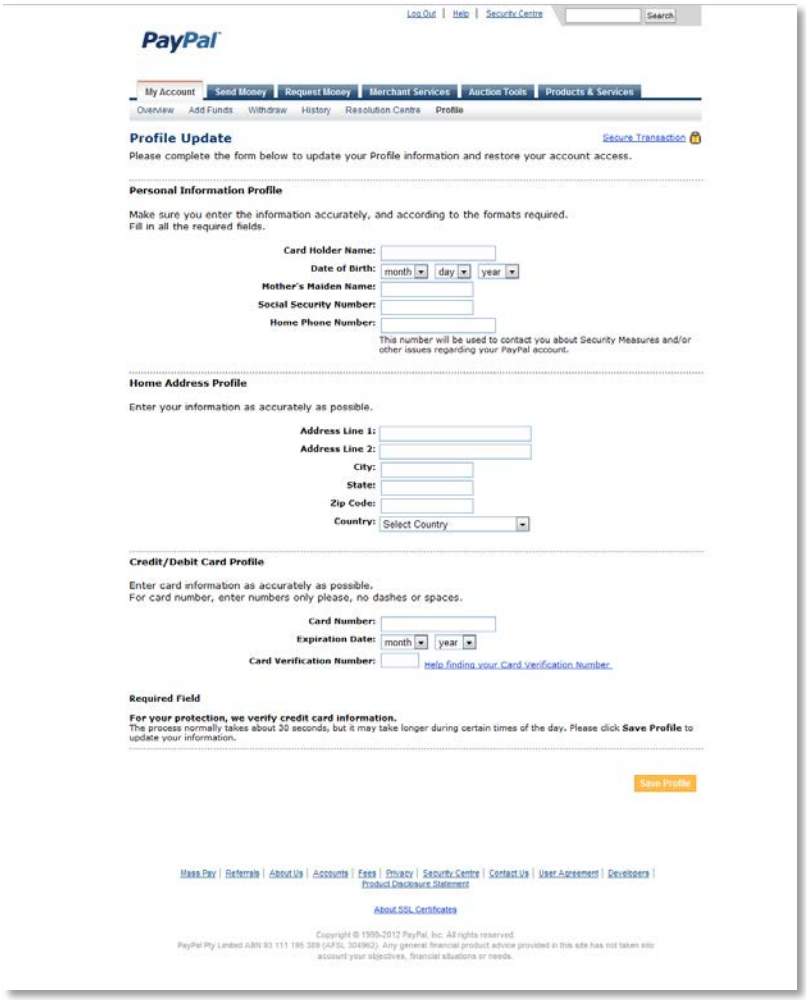
Access to your account was limited for the following reason:

There are activities of which someone tried to access your PayPal account without your permission. To ensure greater security, we have limited access to your account. We have sent you an attachment which contains all the necessary steps in order to restore your account access. Please download and open it in your browser.

(The locator for this issue is **PP-127-311-282**)

We thank you for your prompt attention to this matter. Please understand that this is a security measure intended to protect you and your account. We apologise for any inconvenience.

Sincerely,
PayPal Account Review Department



PayPal

My Account | Send Money | Request Money | Merchant Services | Auction Tools | Products & Services
Overview | Add Funds | Withdraw | History | Resolution Centre | Profile

Profile Update

Please complete the form below to update your Profile information and restore your account access.

Personal Information Profile

Make sure you enter the information accurately, and according to the formats required.
Fill in all the required fields.

Card Holder Name:
Date of Birth: month day year
Mother's Maiden Name:
Social Security Number:
Home Phone Number:
This number will be used to contact you about Security Measures and/or other issues regarding your PayPal account.

Home Address Profile

Enter your information as accurately as possible.

Address Line 1:
Address Line 2:
City:
State:
Zip Code:
Country: Select Country

Credit/Debit Card Profile

Enter card information as accurately as possible.
For card number, enter numbers only please, no dashes or spaces.

Card Number:
Expiration Date: month year
Card Verification Number:
Help finding your Card Verification Number

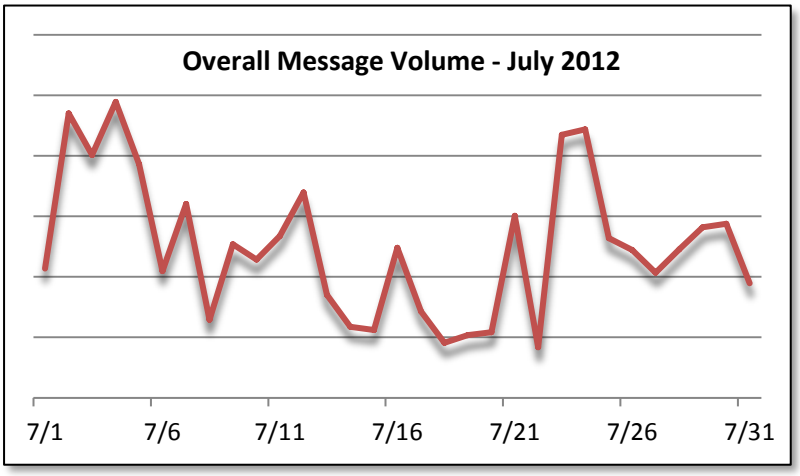
Required Field

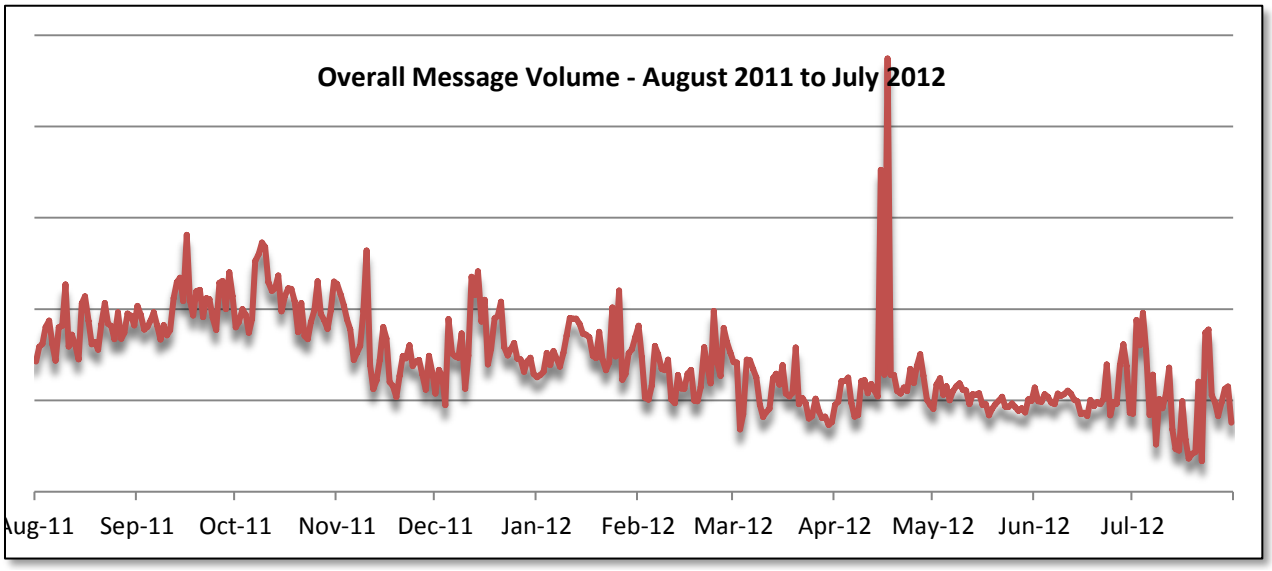
For your protection, we verify credit card information.
The process normally takes about 30 seconds, but it may take longer during certain times of the day. Please click **Save Profile** to update your information.

Save Profile

Spam Volume Trends（スパム量の変化）

スパム量は 2011 年 8 月の水準に比べて 50%ダウンしていますが、この傾向は 5 月にも 6 月にも見られました。Grum ボットネットの解体は 7 月中旬に一時的な影響を及ぼしましたが、平均的なスパム量は 6 月に比べてほぼ同じ(4%減)でした。

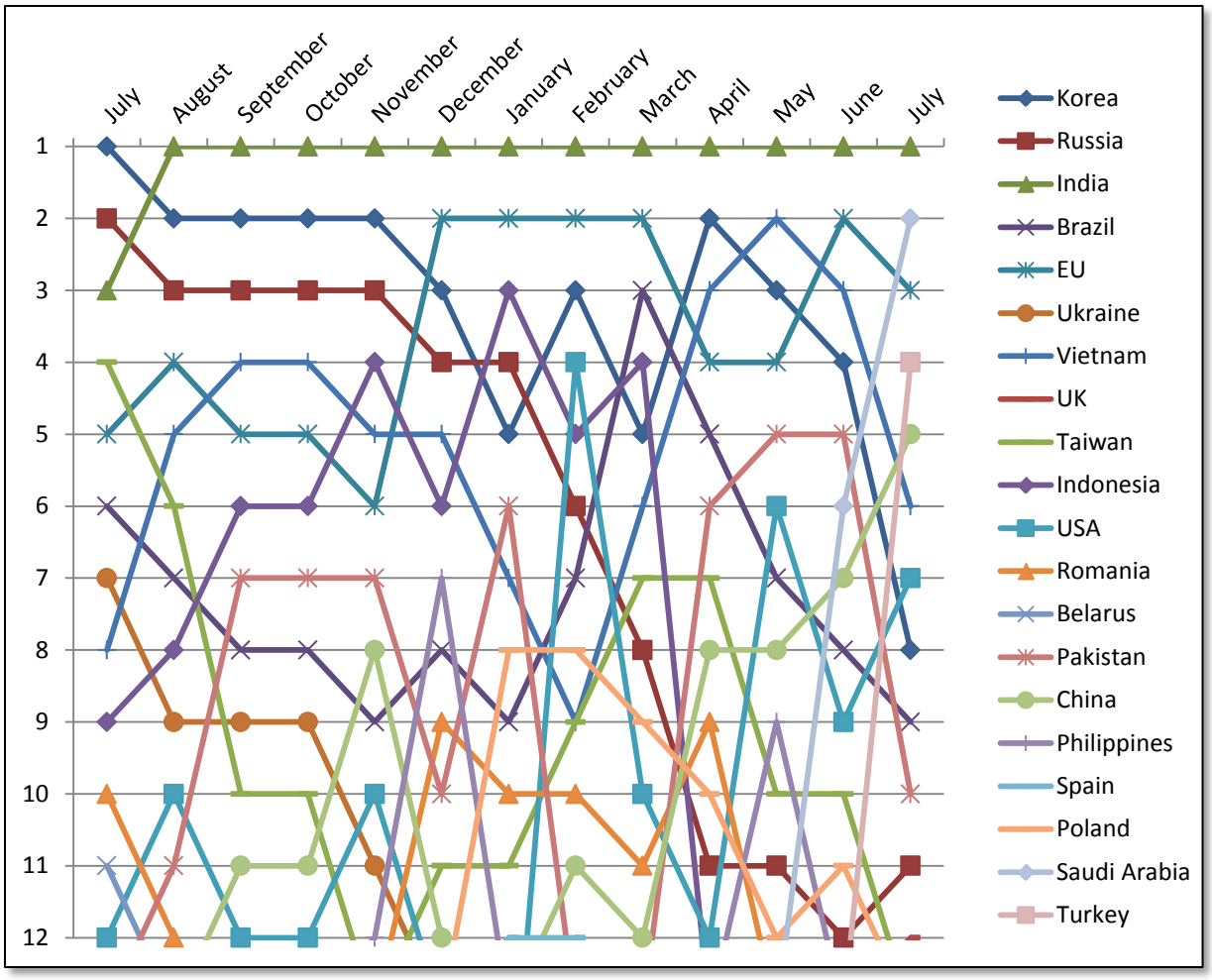




Source of Spam（スパム発信源）

インドが今月も世界一のスパム発信源となっており、2011 年 8 月からの首位を維持しました。しかし、2 位のサウジアラビアとの差は僅少です。サウジアラビアは先月のレポートで始めてランクインしましたが、今月すでに 2 位になりました。このほかでは、トルコが始めて 4 位にランクインしました。

Top Spam Senders by Country											
1	India	**3**	EU	**5**	China	**7**	USA	**9**	Brazil	**11**	Russia
2	Saudi Arabia	**4**	Turkey	**6**	Vietnam	**8**	Korea	**10**	Pakistan	**12**	UK



Language Effectiveness（言語別防御効果）

次のグラフは、Proofpoint ソリューションのスパム防御の有効性を言語毎に示したものです。