電子メール脅威調査レポート

2012 Jul.-Sep.

Cyber Solutions

サイバーソリューションズはアジア地域を重点に、2012 年第三四半期において電子メールに対する脅威を研究及び調査を行いました。

スパムメールの発生元

日本、台湾、中国に送られてきたスパムメールを対象に IP の分析を行った結果、中国 23%、インド 11%、日本 10%がスパムメールの発生元のトップ 3 ということがわかりました。また、一位の中国と二位のインドの差が 12%もありました。

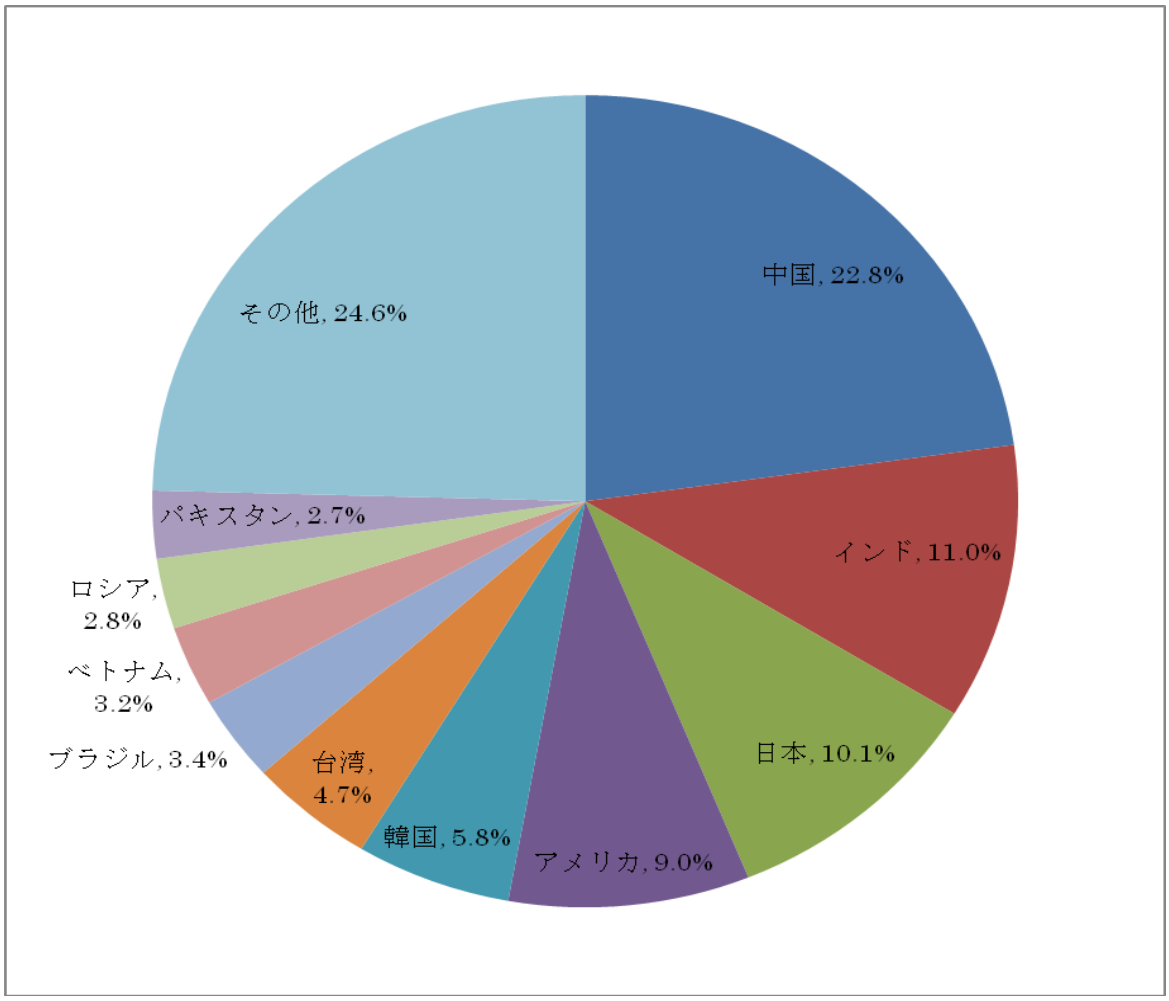


図 1.スパムメールの発生元分布状況

そして、統計データの詳細からみると、八月、九月に中国から配信されたスパムメール量が大幅に増加し、インドと日本の数値が相対的に減少しました。他の国はあまり変化がありませんでした。

國家	七月	八月	九月	平均
中国	18.5%	25.1%	24.9%	**22.8%**
インド	15.6%	10.2%	6.8%	**11.0%**
日本	14.6%	7.4%	8.3%	**10.1%**
アメリカ	9.8%	8.8%	8.3%	**9.0%**
韓国	3.1%	5.7%	8.8%	**5.8%**
台湾	3.2%	5.5%	5.4%	**4.7%**
ブラジル	2.5%	3.6%	4.2%	**3.4%**
ベトナム	4.0%	3.0%	2.4%	**3.2%**
ロシア	1.9%	3.2%	3.2%	**2.8%**
パキスタン	5.8%	1.5%	0.7%	**2.7%**
その他	20.9%	25.9%	27.0%	**24.6%**

表 1. スパムメールの発生元比率ランキング

スパマーがゾンビ PC などの手法により、IP 元を中国に変換してスパムメールを配信したから、表 1 の統計データの結果になったと考えられます。または、最近中国の経済状況が継続的成長し、創業初期の企業も増えてきているため、市場開拓でスパムメールを大量に配信した可能性も考えられます。もちろん、ほかの原因もあると思います。今は、確実な理由がまだ判明できないのですが、弊社は引き続き観察と監視を行い、そして、独自技術により新たな脅威により迅速に対応し、MailGates を利用していただいているユーザー様をお客様のメール環境を守ります。

スパムメール種類

2012 年第 3 四半期には電子メールの本文に含まれる外部リンクを使った攻撃が多く見られます。

また、スパムメールの種類のトップ 3 が以下となります：

表 2. スパムメール種類ランキング

順位	スパムメール種類	比率
1	リダイレクト手法（Redirect）による悪意のサイトへの誘導	30.5%
2	著名 SNS サイトになりすまし、ニセのお知らせメール	13.8%
3	内容不明な添付ファイル	8.8%

各種類を簡単に説明します：

- **リダイレクト手法（Redirect）による悪意のサイトへの誘導：**

  悪意のある外部リンクを正常なリンクに見せかける為、メール本文に短縮 URL やリダイレクトなど様々な方法を利用し、利用者を悪意のサイト誘導する手法が特徴です。

ハッカーが個人情報を取得するための手口が日々変化しています。

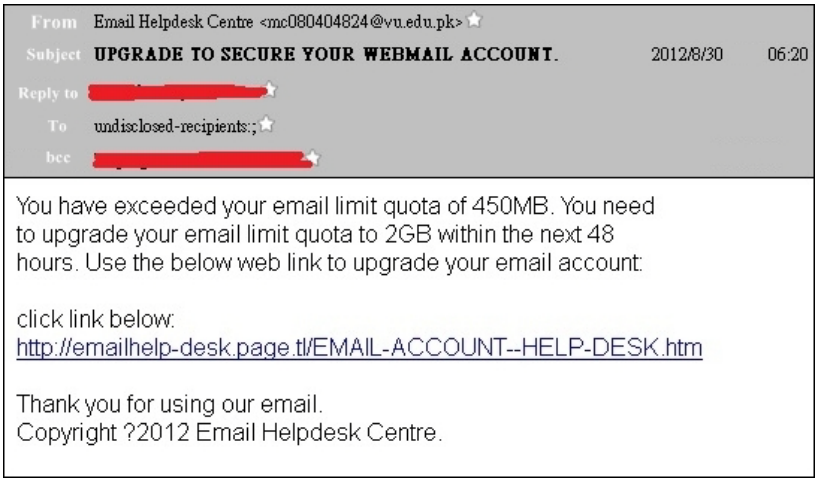
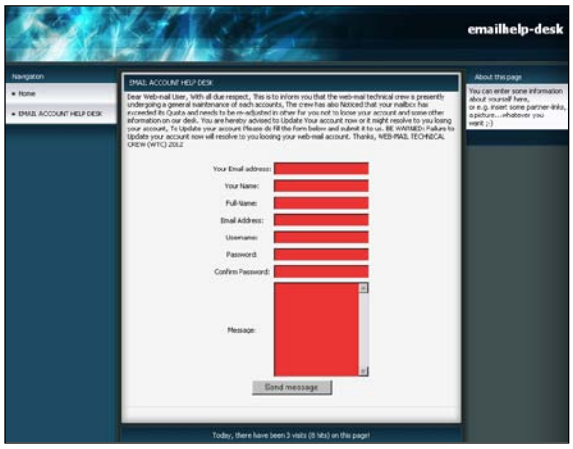


図 2.Email サービスセンターをなりすましたフィッシングメール

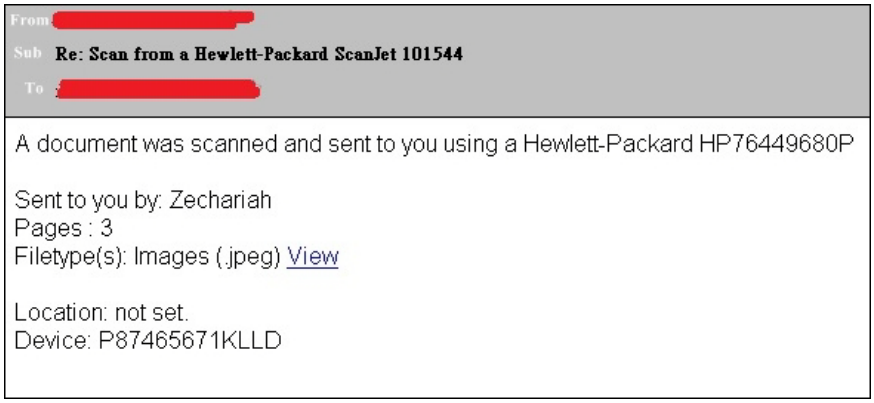
図 2 は、スパマーがメール BOX の容量制限をオーバーしたため、アップグレードが必要との内容でユーザーのアカウント情報を取得する手口の一例です。よく見ると、送信者のドメインは vu.edu.pk なのに、外部リンクのドメインは emailhelp-desk.page.tl になっています。両者は明らかに違います。



さらに、page.tl にアクセスすると、また www.own-free-website.com に誘導され、アカウントとパスワードを入力する無料 WEB サイトの申込画面が表示されたため、このメールは悪意のフィッシングメールに間違いありません。

図 3 サービスセンターのニセログイン画面

図 4 偽造の HP ドキュメント通知メール



第 2 四半期によく出回っていたニセ HP 通知メールは今四半期もやや多くなってきました。メール本文に含まれた外部リンクをアクセスすると、最初に” Please wait a moment. You will be forwarded...”などの内容が表示されると同時に.ru のサイトへ遷移しています。遷移先の広告サイトを強制閲覧させるため、離脱しにくいようにポップアップが多めに表示される仕組みとなっています。

また、世の中、アダルト系のスパムメールもよく出回っています。図 5 がその一例です。この例に要注意な部分は、メール本文中外部リンクです。画面に表示されるリンクの裏にはリダイレクト手法で指定したサイトに遷移するような特別な URL を作成しています。例えば、

http://this-is-a-sample.com/xxxxxxx-yyyyyyyyyy-zzzzzzzzz という URL の xyz 部分を変更すれば、別のサイトに遷移することになります。

図 5　アダルトサイトからのスパムメール

上記のスパムメールの共通点は外部リンクを使って、広告宣伝、利用者のアカウントの取得、または悪意のプログラムを流布させることが目的です。

- **著名 SNS サイトになりすまし、ニセのお知らせメール**:
  引き続き、前四半期と同様に、著名な SNS サイト（Facebook 、Google+、・・等）を利用してスパムを配信することが観測されました。悪意な攻撃をされないように、SNS からの通知メールには注意が必要です。

そして、セキュリティに関わる悪意スパムメール以外、純粋な広告宣伝目的のスパムメールも存在しています。今季も同じく、著名 SNS サイトからのスパムメールが観測されました。

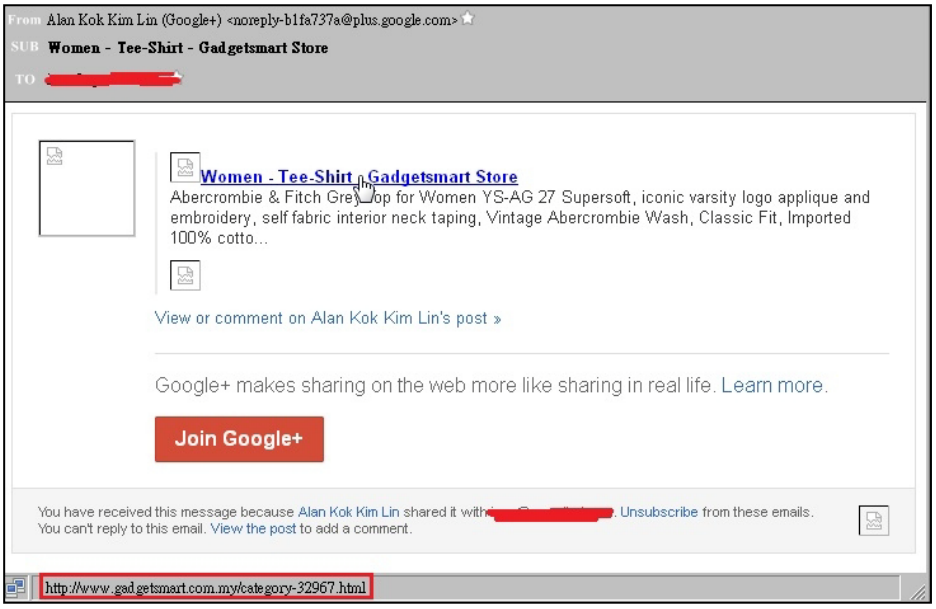


図 6 のように、Google+からの招待状に見えるのですが、実際はマレイシアの某 EC サイトからの広告宣伝メールです。本文中に広告の内容とサイトのリンクが含まれています。

図 6　Google+名義を利用して広告宣伝スパムメール

もちろん、広告スパムメール以外にも、悪意プログラムや外部リンクを含まれたスパムメールがあります。図 7 は LinkedIn からの招待状になりすましたLinkedIn と関係ないサイトに誘導する内容です。

さらに、JavaScript の裏では利用者のパソコン内のデータ収集や悪意プログラムをインストールといった手法は最近よく使われているので、ページのソースに格式一致なコードが大量にあった場合、あるいは、URL をクリックすると”Please wait a moment. …“がしばらく表示され、ページの遷移がない場合も、悪意のある外部リンクをクリックした可能性があります。

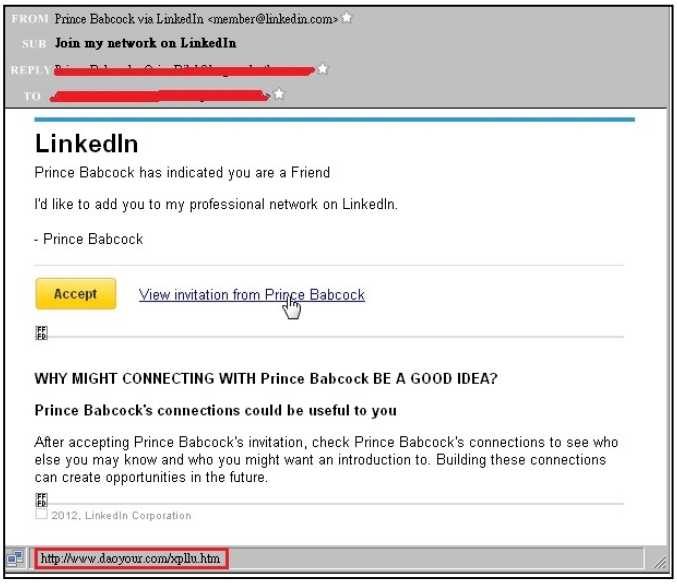


図 7　LinkedIn をなりすました悪意のあるメール

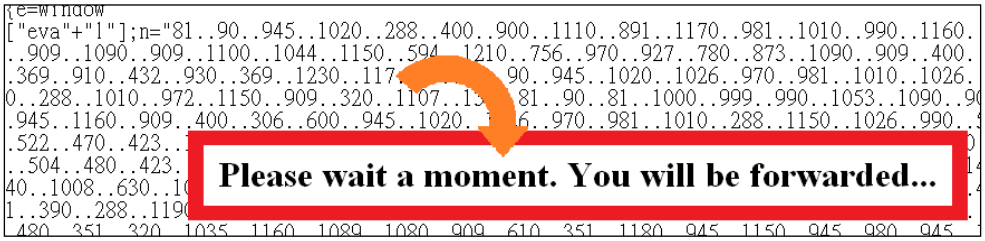
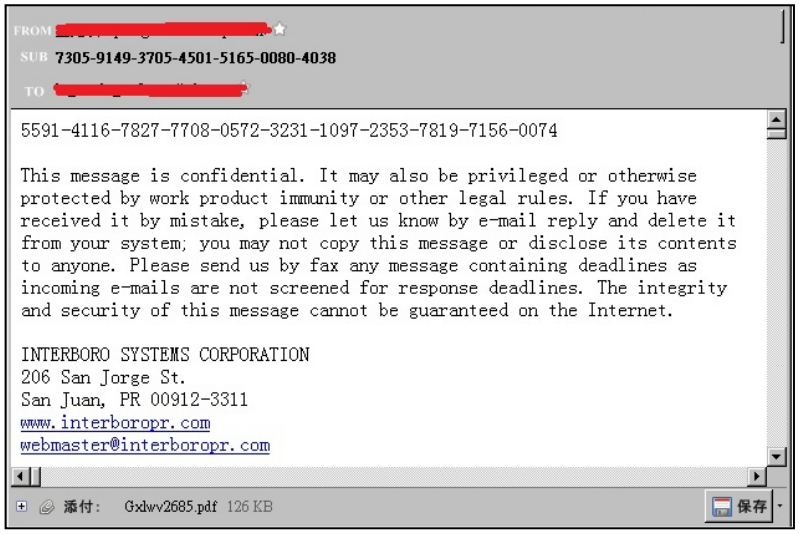


図 9　ソースコード画面

- **内容不明な添付ファイル付きメール:**
  外部リンクが含まれるスパムメールのほか、最近は添付付きのスパムメールも多くなってきています。主に word 文書ファイルや winrar 圧縮ファイルに悪意なプログラムが含まれています。このような疑わしいメールを受信した時に、添付を開かないように注意してください。



そのほか、最も危険なのは不明な添付ファイル付きのメールです。その不明な添付ファイルを開いたと同時に被害を受けた可能性があります。図 8、メール本文中に長い列の数字、機密文書声明、署名、と pdf の添付しかない、意味不明なメールです。そして、その添付ファイルを開いてみると、単なる塾から広告チラシでした。悪意プログラムは含まれていないのですが、スパマーが利用者に添付ファイルを見させることができて、広告スパムが成功しました。

図 9　不明な添付ファイル付きメール

第三四半期中に収集したスパムは、セキュリティに関わる悪意のメール件数と迷惑メール、スパムメール件数の比率は大した変化がありませんが、小さな手口で利用者を騙すことが頻繁にあるので、メールに含まれたハイパーリンクや添付ファイルをより注意深く確認することで被害の危険性を回避できます。

サイバーソリューションズは 2012 年第三四半期の研究及び調査結果の中から、皆様が今後メールをより安全にご利用頂ける様、注意点をご報告させて頂きました。前述のような悪意のメールは、弊社独自技術にて自動検出し、メールセキュリティソリューション MailGates のスパム防御機能に既に反映されております。MailGates では新たな脅威により迅速に対応し、お客様のメール環境を守ります。

【MailGates について】

MailGates は誤送信防止から、スパム対策、メール暗号化まで、メールセキュリティに欠かせない機能を実現に、ウェブインターフェイスによる簡単設定機能など企業に求められる機能を網羅しているメールセキュリティソリューションです。さらに、独自のメールセキュリティテクノロジーとRPD（オンライ検閲機能）の融合且つ高性能多層フィルター。また、Commtouch Software社RPD、Zero-Hourウイルスプロテクションを標準搭載しておりますので、世界各国で飛び交うメールをリアルタイムで監視し新種のスパム、ウイルス、スパイウェア、フィッシングテクノロジなど包括的なマルウェア対策として、的確に排除することが可能になります。http://www.cybersolutions.co.jp/products/mailgates/

【サイバーソリューションズについて】

サイバーソリューションズ株式会社は電子メールサーバをはじめ電子メールセキュリティ関連の製品を中心に、企業向けソフトウェアの開発、販売、提供をしています。

電子メールソリューションの分野におきましては、国内で約 9,500 社以上の企業で利用されている高性能 Web メール機能搭載の統合型セキュア・メールサーバシステム「CyberMail」、内部統制・コンプライアンス対策として国内メーカー実績 NO.1（※）のメール監査・メールアーカイブシステム「MailBase」、未知のスパムも情報漏洩の脅威からも高い投資対効果でシャットアウトできるアンチスパムシステム「MailGates」を開発、販売しております。2009 年より自社の電子メールシステムの技術をクラウド･SaaS 型の「CYBERMAIL∑」提供するサービス事業も開始しました。（※）富士キメラ総研「2012 ネットワークセキュリティビジネス調査総覧」より。

日本の企業では珍しい独自のメールシステムの技術を有することにより、安全で快適な電子メール環境のトータルソリューションの提供を行っています。 http：//www.cybersolutions.co.jp。