



配信不能レポート (Non-Delivery Report) 悪用の スパムメール拡散が広がっています

現在、新たな手法によるスパムメールの拡散が広がっています。トレンドマイクロでは、発展し続けるスパムメール産業に対抗すべく、新たなフィルタリング技術を逐次投入しています。ここでは、最新の拡散手法とその対策手法についてご紹介いたします。

■スパムメール配信業者の発展

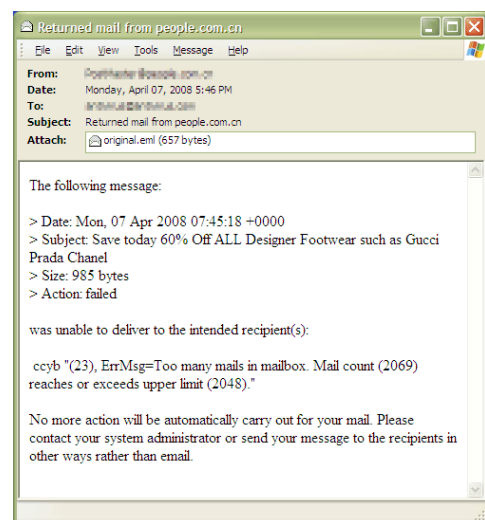
望まない広告の大量配信に端を発するスパムメールは、初期投資の低さから還元率の高いビジネスとして多くの配信業者を生んでいます。それと同時に、望まないメールをブロックしようとする利用者の動きから逃れようと様々なテクニックを生み出しています。スパムメール配信業者の目的は、広告効果すなわち、コンバージョン率(受信者に対し、スパムメールのコンテンツに応じてサイトへ誘導し、実際の取引に結びつける率)を高めていくことです。しかしながら、メール利用者のリテラシー向上、スパムメール対策製品の技術革新などにより、多くのスパムメールは受信者に読まれることなく消えていきます。このような状況において2008年4月に報告されたのが、「後方散乱(Backscatter)メール」として送信される配信不能レポート(NDR:Non-Delivery Report)書式を悪用したスパムメールです。

■配信不能レポート (NDR : Non-Delivery Report) スパムメール

メールプロトコル:SMTP 技術の標準を定めた文書 RFC 2821では、SMTPサーバのメールリレーにおいて、宛先の誤り / 何らかの理由により配信不能であった場合、配信不能レポート:NDRを作成し、送信元にNDRを送信するように定義されています。この際、一部のSMTPサーバにおいては、NDR内にオリジナルメッセージを添付ファイルとして埋め込むことがあります。メッセージがSMTPサーバから跳ね返されたような様から、NDRをバウンスメール(bounce mail)と呼ぶ場合があります。

スパム配信業者はこの仕組みを悪用します。NDRはメールシステムの円滑な利用を支えるために、必要不可欠な仕組みです。このため、管理者は安易にNDRの配送を停止することはできません。また、NDRを受信したメール利用者は、配送不能原因を探るため、添付されたメールを開きます。

故に、スパム配信業者はNDRを詐称したスパムメールを配信することで、配信広告の閲覧率を高め、コンバージョン率を高めることに成功しています。



NDR スパムメールの例 (NDR レポート内にオリジナルメッセージ: 配信業者が閲覧を望む内容が添付ファイルとして埋め込まれています。)

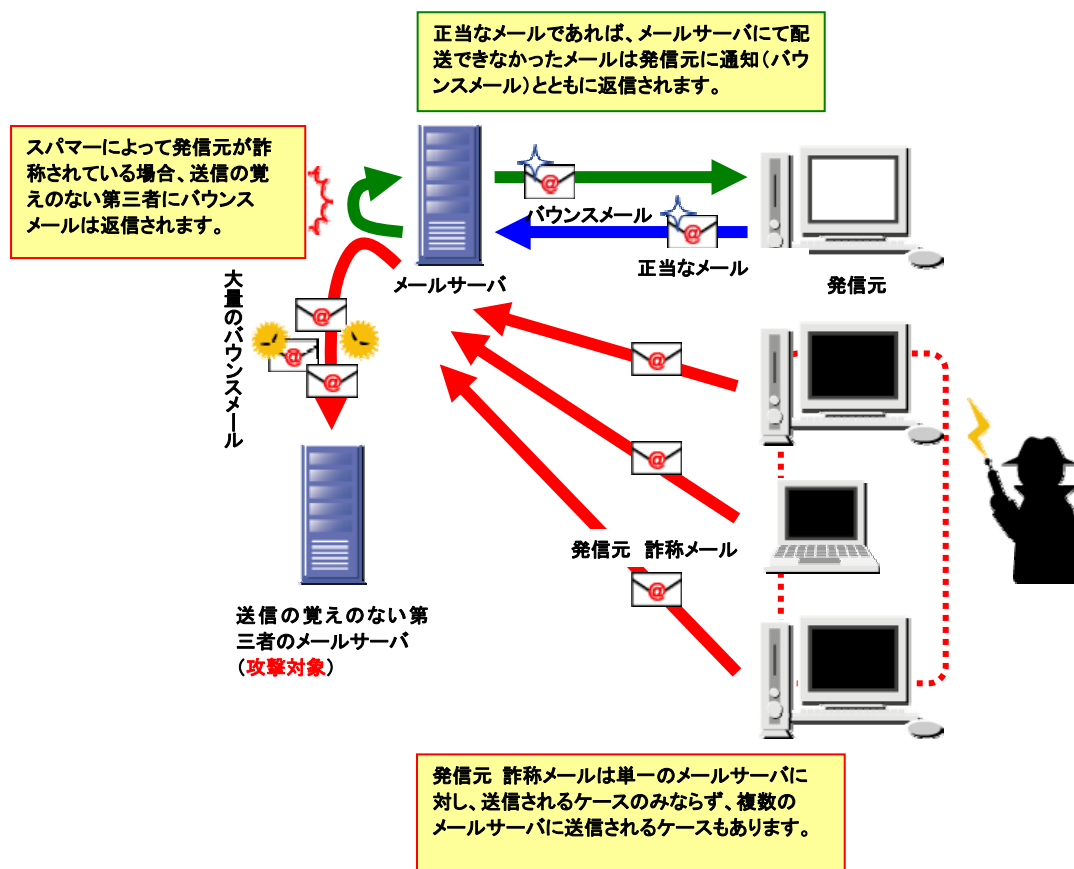
■後方散乱 (backscatter : バックスキャッタ) スпамメール

スパム配信業者が NDR を配信する手口は、自らの手で詐称した NDR を配信するだけではありません。正式な手続きに基づいた NDR すら、悪用の対象としています。後方散乱 (backscatter: バックスキャッタ) メールと呼ばれるその攻撃手法は、被害者のメールサーバ資源を枯渇するだけでなく、被害者が見知らぬ第三者に対し加害者として荷担しうる危険性も挙げられます。

従来、スパム配信業者が NDR の仕組みを悪用した攻撃手法として、DHA (Directory Harvest Attack: ディレクトリハーベスト攻撃) が知られています。これは、メールアドレスの有効性を調査する攻撃手法です。標的組織のメールサーバに対し、自動生成したユーザ名とホストアドレスを組み合わせたメールを大量配信し、NDR の配信 (バウンスメール) 有無を確認することによって、対象メールアドレスの有効性 (バウンスメールが返信されなければ有効なメールアドレス) を確認します。

昨今報告されている後方散乱メールでは、更に巧妙な手口が用いられています。標的組織において無効と確認されたメールアドレスを送信先 (To) に設定し、送信者 (From) もしくは返信先 (Reply-To) に標的組織の有効なメールアドレスを設定します。スパム配信業者によって細工されたメールを受け取ったメールサーバは、無効な送信先が設定されているため、NDR を送信者 (From) もしくは返信先 (Reply-To) に返信を試みます。こうして、返信先には信頼されるメールサーバから送られた NDR として、スパム配信業者が送信するオリジナルメッセージが添付ファイル化され、配信されることとなります。

スパム配信業者が返信先として設定するメールアドレスは NDR を配信するメールサーバと同一組織であるとは限りません。NDR を配信するメールサーバとは異なる組織のメールサーバに対し、大量の NDR 配信を試みている可能性も考えられます。これにより、大量の NDR 配信によりメールサーバ資源の枯渇という被害を受けている被害者が、見知らぬ第三者に対する DoS (Denial of Service: サービス不能) 攻撃の加害者になりうる脅威が発生します。大量の NDR を受け取った被害者の非難の矛先は同じく被害者である NDR 配信メールサーバ所属組織に向けられることとなります。こうして、スパム配信業者は自らの手を汚すことなく、悪意ある活動を継続することが可能となります。



※TRENDMICRO、ウイルスバスターはトレンドマイクロ株式会社の登録商標です。

※各社の社名および製品名は、各社の商標または登録商標です。

Copyright (c) 2008 Trend Micro Incorporated. All Rights Reserved.

■トレンドマイクロ製品におけるNDR悪用スパムメールの対策

NDRを悪用したスパムメールを防ぐ手法には、次のような手段が挙げられます。

- NDRの配信を一律停止する。
- NDRにオリジナルメッセージを添付せずに配信する。
- スパムメール対策製品のコンテンツ検索技術を使用し、NDRスパムメールの特徴を有するメールをブロックする。

これら対策はその有効性は期待できる一方で、NDR本来の役割を損なう懸念が発生します。このため、トレンドマイクロでは、スパムメール対策製品によるコンテンツ検索技術のみならず、レピュテーション技術による対策を提供しています。

- Trend Micro Email Reputation Services Advancedⁱⁱ
トレンドマイクロが提供する、ネットワーク層のレピュテーションによるスパムメール防御サービスです。

レピュテーション技術によるスパムメール対策では、NDRの配信を停止することなく、スパム配信業者の行う後方散乱メールに対する対策を期待することが可能です。

信頼性の低い接続元からのメールに対してのみ、NDRを返信しないことで、利便性を損なうことのないスパムメール対策技術を提供します。

Trend Micro Email Reputation Services Advancedでは、接続元の信頼性(評価点数の監視および維持)を慎重に行っています。また、リアルタイムのスパムメール対策技術では、ヒューリスティックや複雑なアルゴリズムにリアルタイムの監視を組み合わせることで、疑わしい動作を特定して新たなスパムメールの発信元をブロックしています。

こうして構築されたスパムメール送信元のIPアドレスが納められたデータベースを用いることで、スパムメール送信元との接続そのものを遮断します。遮断の際、接続元にはSMTPのレスポンスコードを返答するため、存在しないユーザ宛のスパムメールに対するNDRを返信することがありません。これにより、NDRの発信数増加によるメールサーバ資源の枯渇や、存在しない返信先に対するNDR送信によるリスクを回避した運用を実現することが可能です。

■新たな脅威の報告にご協力ください：スパムデータベースの開発方法

トレンドマイクロでは、リージョナルトレンドラボをはじめとする機関により新たな脅威情報の収集を行い、逐次データベースの更新を行っています。

お客様の環境において、フィルタで検出されないが、スパムメールと疑われるような場合は、そのメッセージ(メッセージヘッダをすべて含めて)を spam@trendmicro.com まで転送してください。

ⁱ Trend Micro Security Blog : スパムマップ配信国ランキング (2008年4月)

<http://blog.trendmicro.co.jp/archives/1363>

TrendLabs Malware Blog : Backscatter Spam Still Alive

<http://blog.trendmicro.com/backscatter-spam-still-alive/>

ⁱⁱ トレンドマイクロでは、無償で使用できる体験版を提供しています。

<http://www.trendmicro.co.jp/tm/ers-trial/>