一般口演B

[KB15] 一般口演 B
医療機関に向けて送信されたマルウエア感染企図メールおよび金銭目的雑誌投稿勧誘メールの SMTPエンベロープヘッダの特徴解析

2018年6月23日(土) 15:30 ～ 16:00 第1会場 (2階・メインホール)

[KB15] 医療機関に向けて送信されたマルウエア感染企図メールおよび金銭目的雑誌投稿勧誘メールの SMTPエンベロープヘッダの特徴解析

渡辺 淳 （関西医科大学 大学情報センター）

©一般社団法人 日本医療情報学会

KB15

医療機関に向けて送信されたマルウエア感染企図メールおよび金銭目的雑誌投稿勧誘メールの SMTP エンベロープヘッダの特徴解析

渡辺　淳[*1], 仲野　俊成 [*1]
[*1] 関西医科大学　大学情報センター

Signature analysis on SMTP envelope headers of malicious email messages and on the headers of unsolicited email messages from predatory publishers to a medical university

Jun Watanabe[*1], Toshiaki Nakano[*1]
[*1] 1University Information Center, Kansai Medical University

抄録：医療機関のメール受信中継サーバに直近 2 年間で着信した迷惑メール約 220 万通の SMTP エンベロープヘッダの特徴についてデータマイニングを用いて解析し、阻止の方略を検討した．マルウエア攻撃メールは、当初、情報漏洩を企図した snowshoe 攻撃が主で迷惑メールの 5%未満であったが、調査期間終盤には botnet を介するマルウエア攻撃（ランサムウェアを含む）の著増により約 20%に増加した．これらの攻撃では特定の IP アドレス領域からの送信、特徴的な送信者アドレス、不正な helo などの特徴が観察され、それらの特徴を組み合わせたフィルタで大部分を阻止できた．営利目的のハゲタカ（捕食：predatory）出版社からのメールは迷惑メールの約 20–30%を占めた．送信ドメイン所有者の多くは南アジアで、大部分が特定のホスティング業者のサーバ群から送信されていた．送信者アドレスのドメイン部および送信サーバの FQDN または IP アドレス範囲を組み合わせたフィルタによって、それらの 95%以上を阻止できた．

キーワード　迷惑メール、マルウエア、捕食出版社、データマイニング、医療機関

1.　はじめに

近年、ランサムウェアをはじめとするマルウエア添付メールやドライブ・バイ・ダウンロード (Drive-by download：メール記載の悪意あるサイトへのリンクを押させて感染させる) を用いた攻撃が増加しつつある．医療機関は、これらの攻撃による情報漏洩やデータを人質とした「身代金」奪取等の脅威にさらされている．また、医療機関に向けて営利目的の「捕食・ハゲタカ (predatory)」出版社から投稿料奪取を主目的とした多数の迷惑メールが送信されており、業務の妨げとなっている．

本研究では、マルウエア攻撃、および営利目的の捕食出版社からの迷惑メールについて、電子メールの SMTP エンベロープヘッダ情報の特徴を解析して阻止ルールを策定することで、それらを排除するための方略を検討・検証した．

2.　方法

直近 2 年間に医科大学のメール受信中継サーバ群に着信した迷惑メール約 220 万通の SMTP エンベロープヘッダ情報を用いた．SMTP エンベロープヘッダに記載された送信者アカウントのアカウント部とドメイン部、送信サーバの FQDN と IP アドレス、接続時に送信サーバが名乗る helo/ehlo、（以下 helo）および Whois 情報と BGP tool kit [1] で調べた送信元 IP アドレス領域の所有者情報等について、個々の特徴の感度、特異度を調べ、またそれらの相互関係を、おもに中心性指標用したネットワーク分析（実装は KH coder [2]）、複数の特徴を組み合わせた際の信頼度と支持度を Apriori のアルゴリズムを用いたアソシエーション分析によって解析した．それらの結果に基づいて検出ルールを策定し、受信中継サーバの MTA（Postfix）にセットして検出精度を評価した．

迷惑メールか正規（legitimate）メールかの判定は、SMTP ヘッダにおける各項目の記載事項を検索して web site や blog で公開されている情報から判定する手法、および囮アカウントで収集したメールの目視確認を併用した．　マルウエア攻撃の同定には、囮アカウントを用いて捕捉したメールの目視確認および Malware-Traffic-Analysis.net [3] 等に掲載された情報に依った．捕食出版社は

Beall's List の最新または最終版、送信ドメイン登録日と所有者情報、出版社・雑誌の web site、JCR 収載の有無を総合して判定した.

3. 結果

1) マルウエア攻撃メール

マルウエア攻撃メールは、当初、全迷惑メールの 5%未満であったが、調査期間中に増加した. 当初最も多かったのは中国の IT 企業のサーバ群を用いた snowshoe 攻撃(多数の送信サーバを用い、送信サーバを次々と変化させて大量送信を行う)とドライブ・バイ・ダウンロードとを組み合わせた情報漏洩・奪取目的の攻撃で、大手の金融機関や配送業者を詐称した送信者アドレスの多用が見られた. マルウエア添付メールの多くは botnet を介するランサムウェアを含む攻撃で、送信元は、当初、ロシアおよびベトナムが主だったが、その後、中国や東欧にも拡大した. マルウエア攻撃メールでは、偽装された送信者アドレスのドメイン部は送信サーバのドメインと異なり、helo と偽装された送信者アドレスのアカウント部またはドメイン部との間には共起関係((送信者アドレスのドメイン部に rambler.ru が出現すれば特定の helo (例では yandex.ru)が同一ヘッダに出現)が観察された. 以下は送信サーバ FQDN [IP アドレス]、from=<送信者アドレスアカウント部@ドメイン部>、helo=<接続時に名乗る自サーバ名>の例である:

マルウエア(ダウンロータ)攻撃メールの例:
unknown[61.160.112.74]
from=< g.janetta@rambler.ru>
helo=<dtqt.yandex.ru>
マルウエア(ランサムウエア)攻撃メールの例:
unknown[14.168.112.161]
from=< Edna.Mahar@takii.kmu.ac.jp>
helo=<static.vnpt.vn>

これらの特徴を検出するフィルタで攻撃メールの 90%以上を検出可能となり、DNS-BL (zen.spamhaus.org 他)の併用によって 97%以上を阻止できた (DNS-BL のみでは約 80%)が、他機関からの転送メールではすり抜けが発生した.

2) 捕食出版社からの迷惑メール

捕食出版社からの投稿勧誘メールは、当初、迷惑メールの約 10-15%を占め、後に 20-30%に増加した. 2年間に着信した送信者アドレスのドメイン部の総数は 1,500 以上で、それらの多くは直近 2 年以内に南アジアで登録されていた. また、大半が南アジアのホスティング業者の所有する約 40 のドメインから送信され、途中で送信業者を変更・増加させる傾向が観察された. これらの 95%以上は送信者アドレスのドメイン部が送信サーバのドメインと異なっていたが、それらの間に共起関係が観察された. 送信数上位 20 ドメインについては特異度 99.9%以上での検出が可能であり、この結果を反映したフィルタによって 95%以上を阻止した(DNS-BL 単体の阻止率は 10%未満).

4. 考察

国内外の多数の医療機関においてランサムウェアを含むマルウエアを用いた攻撃の被害が報告されている. また、国内からの送信が増加しつつあり、国内の大学・医療機関のドメインや、研究者、医師が用いている個人アドレスの詐称も認められた. 医療期間に属するスタッフの電子メールアドレスの多くは、論文検索サイト等で公開されているため、今後、それらの公開アドレスを用いた攻撃の増加が危惧される.

5. 結語

医療機関を標的とする、ランサムウェアを含むマルウエア攻撃、および捕食出版社からの迷惑メール送信の実態の一端を解明し、SMTP エンベロープヘッダの特徴解析によって、これらの攻撃に使われる迷惑メールの 95%以上を阻止した.

参 考 文 献

[1] Hurricane Electric BGP Toolkit. http://bgp.he.net/ (cited 2018-Feb-1).

[2] 樋口耕一. テキスト型データの計量的分析 -2 つのアプローチの峻別と統合-. 理論と方法, 19, 101-115, 2004.

[3] http://www.malware-traffic-analysis.net (cited 2018-Feb-1)