スパムトラップを用いたマルウェア添付スパムメールの分析

志村 正樹 †　畑田 充弘 ‡　森 達哉 †　後藤 滋樹 †

† 早稲田大学
169-8555　東京都新宿区大久保 3-4-1
{m-shimura,goto}@goto.info.waseda.ac.jp, mori@nsl.cs.waseda.ac.jp

‡NTT コミュニケーションズ株式会社
108-8118　東京都港区芝浦 3-4-1 グランパークタワー 16F
m.hatada@ntt.com

あらまし 近年，スパムメールに添付されたマルウェアによる被害が拡大している．スパムメールに添付されたマルウェアは，Zip ファイルなどに圧縮する，拡張子を文書ファイルのように偽装するなどの手法を用いることで正常なファイルに偽装している．本研究では，スパムメールを収集するためのハニーポットであるスパムトラップに届いたマルウェアが添付されたスパムメールを分析する．本論文ではスパムメールをキャンペーンという単位で扱う．これを用いて，スパムメールに添付されるマルウェアの形式 (Zip，文書ファイル，実行ファイル) ごとに特徴を分析した．また出現回数の多い典型的なスパムの例を提示した．

Analysis of spam mail containing malicious attachments using SpamTrap.

Masaki Shimura†　Mitsuhiro Hatada‡　Tatsuya Mori†　Shigeki Goto†

†School of Fundamental Science and Engineering, Waseda University
3-4-1 Okubo, Shinjuku-ku, Tokyo 169-8555 JAPAN
{m-shimura,goto}@goto.info.waseda.ac.jp, mori@nsl.cs.waseda.ac.jp

‡NTT Communications Corporation
Gran Park Tower 16F, 3-4-1 Shibaura,Minato-ku, Tokyo,108-8118 JAPAN
m.hatada@ntt.com

Abstract In recent years, the damage from malware attached to spam e-mail has been growing. Malware attached to spam mail are disguised as legitimate ones. This paper utilizes SpamTrap which collects spam e-mail message. If the contents of some malware files are identical, these are grouped into a single campaign. We classify attached malware files into zip, documents, and exec files. The analysis is based on the set of campaigns. This paper gives typical example spam messages which are popular among SpamTrap data.

1　はじめに

近年，スパムメールに添付されたマルウェアによる被害が拡大している．スパムメールは主に広告などを目的としたメールであるが，その中にはマルウェア感染を目的とし，マルウェアを添付して送信されるスパムメールが存在する．このようなマルウェアに感染すると，ボットネッ

トとして攻撃に加担させられる，個人情報の流出，他のマルウェアをダウンロードさせられるなどの被害が生じる．このようなマルウェアを添付するスパムメールは，広告などを目的としたものとは性質が異なると考えられる．

そこで本研究では，スパムメールの中でもマルウェアを添付しているものに着目し，その特徴を分析する．

本論文の構成は下記の通りである．はじめに 2 章で関連研究を示す．続いて 3 章はデータ収集環境およびデータの概要を示し，4 章でマルウェアが添付されたメールの分析，及び代表的なマルウェア添付スパムメールの例を示す．最後に 5 章で議論を， 6 章でまとめを述べる．

2 関連研究

本章では，スパムメールに関する既存研究を述べる．スパムメールに関する研究では，スパムメールの分類手法や，スパムメール送信に関わるユーザの分析などの観点から研究が行われている．

Gianluca [1] らは，スパムメールの送信に関わる悪性ユーザに関する分析を行っている．これによれば，スパムの送信にはメールアドレスを収集する Harvester，メール送信に用いる bot を管理する Botmaster，実際にスパムメールを送信する Spammer のユーザが関わるという．

christian kreibich [2] らは，Storm というボットネットから送信されるスパムキャンペーンに着目し，キャンペーンの送信期間やコンテンツの種類などを明らかにしている．この研究ではスパムキャンペーンを単一のテンプレートから作成されるスパムメールとし，その目的やスパムの要素などの観点からキャンペーンを分析している．

本研究では，スパムメール全体ではなく，マルウェアが添付されたスパムメールを対象とし，その特徴の分析を行う．また，添付されるマルウェアに基づいてキャンペーンを分類し，キャンペーンの特徴を分析する．

表 1: スパムトラップに使用されるドメイン数

TLD	com	net	jp	org
ドメイン数	62	23	5	1

3 データ収集環境およびデータの概要

3.1 データ収集環境

本研究ではスパムメールのみを収集するメールサーバであるスパムトラップを設置･運用して電子メールの定点観測を行った．スパムトラップは一般の用途で使用されていないメールアドレスに届くメールを収集する．そのためスパムトラップに送信されるメールは，スパムメールなとの悪性のメールと考えられる．本実験に用いたスパムトラップでは，合計で 91 のドメインを利用してスパムメールの収集を行った．表 1 に本実験で用いたドメイン数をトップレベルドメインごとに示す．

3.2 データの概要

本実験では，スパムトラップを用いて 2013 年 10 月から 2015 年 7 月に送信されたスパムメールを収集し分析対象とした．収集されたスパムメールの中から，文書ファイル (PDF,Microsoft Office 文書)，実行ファイル，および zip ファイルを添付ファイルとして持つメールを抽出した．この添付ファイルを，オンラインのファイルスキャンサービスである VirusTotal [3] を用いてスキャンし，5 種類以上のアンチウイルスソフトでマルウェアと判定された場合，マルウェアであるとの判定を行った．そしてマルウェアであると判定された同種類の添付ファイルを持つスパムメールを，同じコンテンツをもつスパムメールであるとして，同じキャンペーンとして分類し，分析を行った．

観測期間における全受信メール数，添付ファイル付き電子メール数，マルウェア添付ファイル付き電子メール数の合計を表 2 に示す．また，各月ごとの受信メール総数，添付ファイル種別のメール数の遷移を図 1 に示す．2014 年 9 月

表 2: 観測期間全体のメール数

	メール数
全受信メール	30,193,779
添付ファイル付き電子メール	422,594
マルウェア添付ファイル付き電子メール	363,042

表 3: マルウェア種別ごとのメール数

	メール数
Trojan	184,011
Upatre	103,669
Zbot	72,848
Mydoom	2,355
other	122

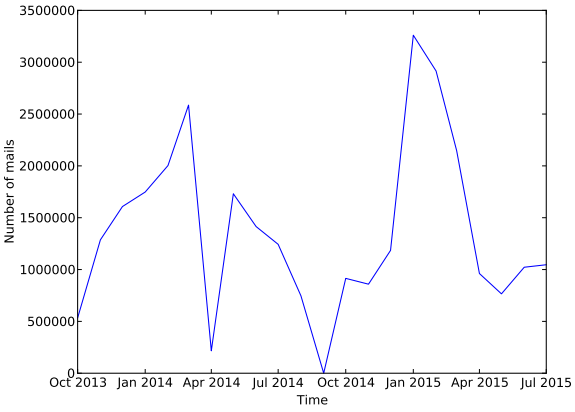

図 1: スパムメール数の時系列変化

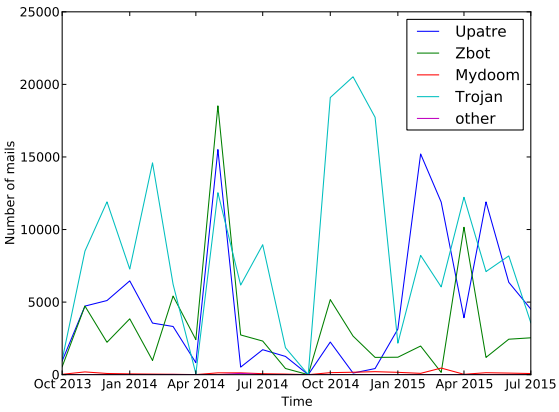

図 2: マルウェア数の時系列変化

にはスパムメールの収集が出来なかったためにデータが欠損している．

VirusTotal を用いて分類した，観測期間全体のマルウェアの種別ごとのメール数を表 3 に，月ごとのマルウェア種別ごとのメール数を図 2 に示す．本実験では，マルウェアを Mydoom，Upatre，Zbot，Trojan，other の 5 種類に分類した．Mydoom [4] はスパムメール送信機能を持つワーム型のマルウェアであり，感染した端末から自身のコピーを送信することで感染を拡大する．Upatre [5] はトロイの木馬型のマルウェアであり，感染すると内部で複製され，さらなる不正ファイルのダウンロードと実行を行う．Zbot [6] は銀行取引などの個人情報を盗み出すことを目的としたトロイの木馬である．Trojan はその他のトロイの木馬型のマルウェア，other は Mydoom，Upatre，Zbot，Trojan のいずれとも判定されなかったマルウェアである．Mydoom などのワーム型のマルウェアよりも，さらなるマルウェア感染や情報収集に繋げるためのトロイの木馬型のマルウェアが主流となっていることが分かる．

3.3 スパムキャンペーンの分類

本実験では，スパムメールの subject，および添付ファイル名の特徴を用いてスパムメールをキャンペーンに分類した．同一のキャンペーンでは同種類のマルウェアが使用されるが，ハッシュ値による検出を逃れるために同一のキャンペーンでもマルウェアのハッシュ値が異なる場合がある．そこで本実験では 48 時間以内にマルウェアの種類が同一かつ，以下のいずれかの特徴を持つスパムメールが複数観測された場合，それらのメールは同一のキャンペーンであると判定した．

1. subject，または添付ファイル名が同一
2. subject，または添付ファイル名が単語＋ランダムな英数字列となっており，単語部分が一致

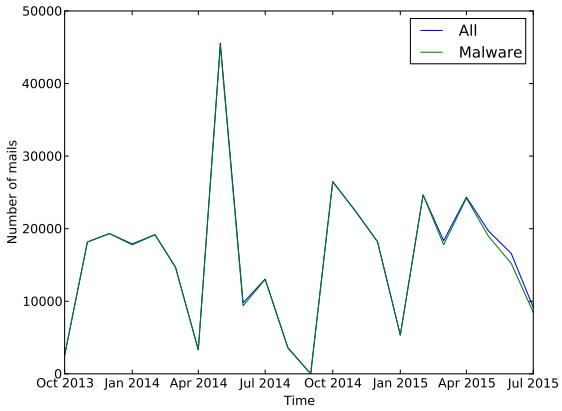

図 3: Zip ファイル形式のメール数

表 4: 圧縮ファイルの拡張子 (上位 5 件)

拡張子	メール数
exe	269408
scr	64244
js	4084
zip	659
html	622

4 マルウェア添付メールの分析

4.1 Zip ファイル形式

4.1.1 メールの分析

Zip ファイル形式のマルウェアが添付されたスパムメールの特徴を分析する．Zip ファイルが添付されたメール数および，マルウェアと判定されたメール数の時系列変化を図 3 に示す．図 3 において 2 つのグラフが重なることから，スパムメール上で観測される多くの Zip ファイルがマルウェアであることが分かる．

表 4 に，Zip ファイルに圧縮されていたファイルの拡張子の上位 5 件を示す．ここから，多くのの Zip ファイル形式のマルウェアは文書ファイルなどを用いず，exe や scr などの実行ファイルを直接圧縮している場合が多いことが分かる．また Zip ファイルをさらに Zip 圧縮したものも一定数確認された．また，マルウェア種別ごとのメール数を表 5 に示す．多くはトロイの木馬と Upatre，Zbot などのトロイの木馬であることが分かる．

表 5: Zip ファイル形式のマルウェアの種類

マルウェア種別	メール数
Trojan	169,078
Upatre	103,440
Zbot	72,786
Mydoom	1,924
other	121

4.1.2 キャンペーンの分析

スパムメールをキャンペーンに分類した結果の特徴を示す．Zip ファイルのキャンペーン数の累積分布を図 4 に示す．3 割超のキャンペーンが 1 通のメールのみのキャンペーンと判定され，本研究に用いたデータでは同一の内容のメールが発見されなかったことが分かる．一方 1000 通を超えるキャンペーンも存在し，キャンペーンの規模に大きな差があることが分かる．また，メール数が 5 通以上のキャンペーンに対し，メール数とユニークな送信先ドメイン数の関係を図 5 に示す．メールの送信規模に対して対象となるドメイン数も増加していることが分かる．

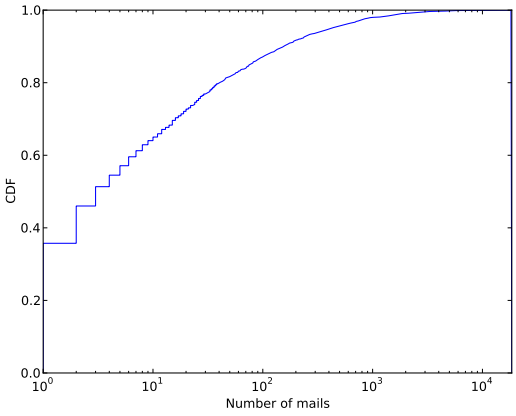

図 4: Zip マルウェアキャンペーンのメール数の累積分布

4.1.3 スキャナからのメールに偽装したメールの例

Zip ファイル形式のマルウェアが添付された例の一つとして，スキャナからのメールを装ったメールの例を示す．これはスキャナから送信

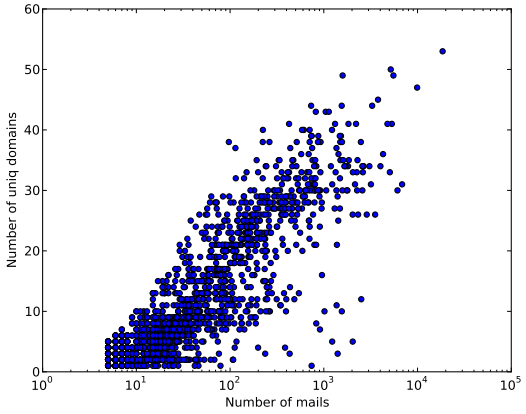

図 5: Zip マルウェアキャンペーンのメール数とユニーク送信先メイン数の関係

されるスキャンデータを格納した Zip ファイルを装って送信されるスパムメールである．

> Subject: Scanned Image from a Xerox WorkCentre
>
> You have a received a new image from
> Xerox WorkCentre.
>
> Sent by: XXXXXX.com
> Number of Images: 8
> Attachment File Type: ZIP [PDF]
>
> WorkCentre Pro Location: Machine location not set
> Device Name: charmedmail.com
>
> Attached file is scanned image in PDF format.
> Adobe(R)Reader(R) can be downloaded
> from the following URL: http://www.adobe.com/

subject は実在するスキャナの名称を騙っている．本文では画像の数や実在する URL などを表示させ，正規のメールであるように見せている．本メールに添付されている Zip ファイル名は Scan001_3884976_008.zip となっており，スキャンデータのようなファイル名となっている．圧縮されているファイル名は Scan001_0047039_008.scr という実行ファイルになっており，Upatre と判定されたマルウェアであった．

4.2 文書ファイル形式

4.2.1 メールの分析

文書ファイル形式のマルウェアが添付されたスパムメールの特徴を示す．文書ファイルが添付されたメール数及び，マルウェアと判定されたメール数の時系列変化を図 6 に示す．文書ファイルの場合，マルウェアである確率は Zip ファイルなどに比べて低い事がわかる．これはスパムメールにおいて文書ファイルは詐欺や広告など，マルウェア以外の目的にも用いられためだと考えられる．しかし 2015 年付近から，文書ファイル形式のマルウェアが占める割合が増加していることが分かり，2015 年の 7 月には約半数がマルウェアという結果となった．これは 2014 年の 12 月から急増した，Microsoft Office のマクロ機能を悪用してマルウェアに感染させようとする手口 [7] によるものと考えられる．また，マルウェア種別ごとのメール数を表 6 に，ファイルの拡張子ごとのメール数を表 7 に示す．文書ファイル形式は，ほぼすべてのメールがトロイの木馬であることが分かる．また，拡張子はほとんどが doc であり，Word 形式のファイルが多く使用されていることが判明した．

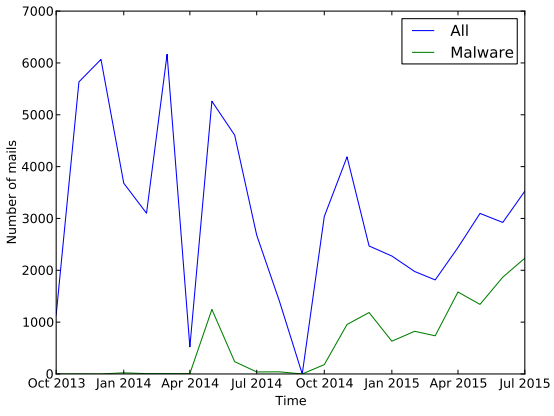

図 6: 文書ファイル形式のメール数

4.2.2 キャンペーンの分析

キャンペーンごとに分類した結果の特徴を示す．文書ファイルのキャンペーン数の累積分布

表 6: 文書ファイル形式のマルウェアの種類

マルウェア種別	メール数
Trojan	12,889
Upatre	213
Mydoom	33
Zbot	4
other	0

表 7: 文書ファイル形式のマルウェアの種類

拡張子	メール数
doc	11,175
pdf	1440
xls	480
docx	25
xlsx	19

を図 7 に示す．Zip ファイルと同様に，3 割程度のキャンペーンのメール数が 1 と判定されている．キャンペーンの規模は最大でも 1000 通未満であり，Zip ファイルに比べてキャンペーンの規模は小さい傾向がある．また，メール数が 5 通以上のキャンペーンに対し，メール数と送信先ドメイン数の関係を図 8 に示す．Zip ファイル同様に，メールの送信規模に対して送信先の対象となるドメイン数も増加していることが分かる．

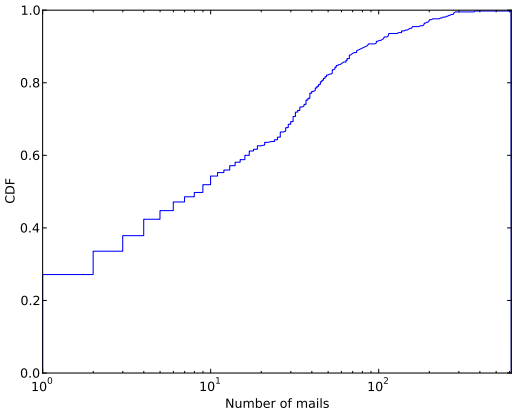

図 7: 文書マルウェアキャンペーンのメール数の累積分布

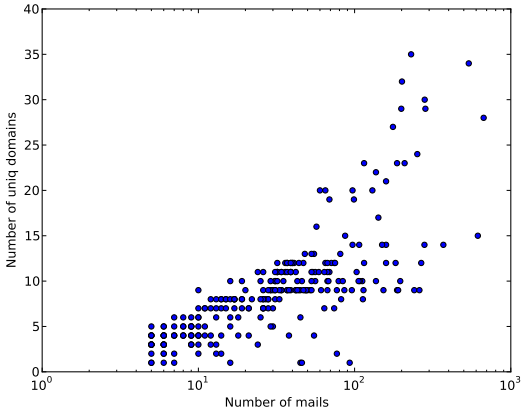

図 8: 文書マルウェアキャンペーンのメール数とユニーク送信先ドメイン数の関係

4.2.3 請求書に偽装したメールの例

文書ファイル形式のマルウェアが添付された例として，請求書に偽装したマルウェアの例を示す．

> Subject: Invoice information
>
> You have received the bill !
> Received at: Tue, 28 Jul 2015 16:09:19 +0000.
> Number of pages: 7.
> Dispatcher Identification: 700.
> Delivery order: 5753758707.
> Kindly be advised that applied is copy of the first page only.
> We will forward the hard copies to You at the location
> stated already.

配送番号や日時などが本文に記述され，業務で使用されるメールのような本文となっている．本メールに添付されているファイル名は Invoice_#_5753758707-adyNw.doc という Word ファイルで，マルウェアの種類はトロイの木馬である．このように，文書ファイル形式では業務で使用されるメールに偽装されたものが多く確認された．

4.3 実行ファイル形式

4.3.1 メールの分析

実行ファイル形式のマルウェアが添付されたスパムメールの特徴を示す．実行ファイルが添

付されたメール数及び，マルウェアと判定されたメール数の時系列変化を図 9 に示す．図 9 より，実行ファイルはメール数は少ないものの，殆どの場合がマルウェアであると分かる．

また，マルウェア種別ごとのメール数を表に示す．実行ファイル形式では，Zip ファイル形式や文書ファイル形式の場合に比べて Mydoom の割合が大きい．これは Mydoom が自身のコピーを送信する性質を持つため，exe 形式で送信される Mydoom が多いためと考えられる．

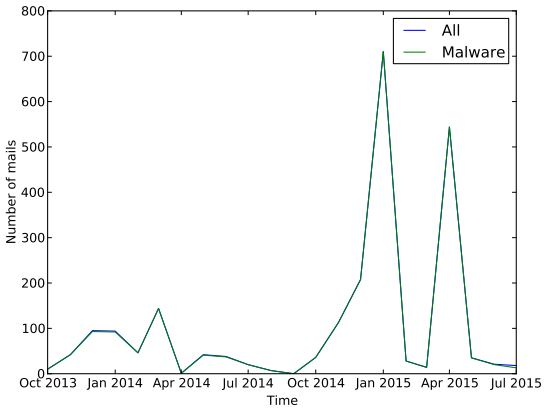

図 9: 実行ファイル形式のメール数

表 8: 実行ファイル形式のマルウェアの種類

マルウェア種別	メール数
Trojan	1,583
Mydoom	398
Zbot	58
Upatre	16
other	1

4.3.2 キャンペーン単位の分析

実行ファイルのキャンペーン数の累積分布を図 10 に示す．6 割以上のキャンペーンのメール数が 1 であると判定され，ほぼすべてのキャンペーンのメール数が 100 通以下である．これより，実行ファイル形式のマルウェアはキャンペーン単位ではなく，単体のメールで送信されることが多いことがわかる．

また，メール数が 5 通以上のキャンペーンに対し，メール数と送信先ドメイン数の関係を図 11 に示す．

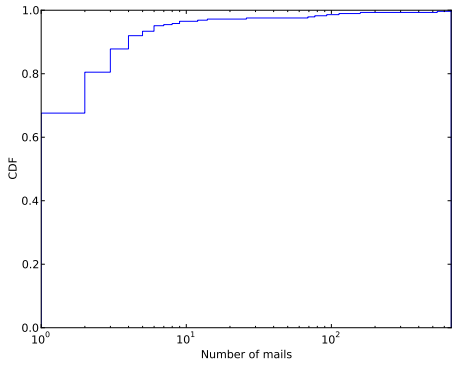

図 10: 実行ファイル形式マルウェアキャンペーンのメール数の累積分布

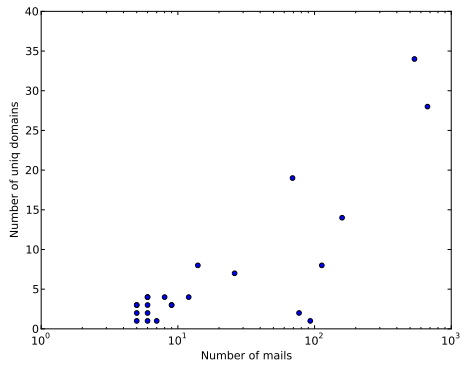

図 11: 実行ファイル形式マルウェアキャンペーンのメール数とユニーク送信先メイン数の関係

4.3.3 請求書に偽装したメールの例

実行ファイル形式のマルウェアが添付された例として，エラーメールに偽装した例を示す．

> From: ”The Post Office” MAILER-DAEMON@xxxxxxxx.net¿
>
> Subject: Mail System Error - Returned Mail
>
> The original message was included as attachment.

このメールの送信元アドレスのローカル部が MAILER-DAEMON となっており，送信エラー

による自動返信メッセージのように偽装している．添付ファイルは document.exe という実行ファイルで，マルウェア種別は Mydoom となっている．

5 議論

本実験の課題などについて述べる．本実験ではスパムメールから添付ファイルを抽出し，その添付ファイルを VirusTotal を用いて分類し，その結果に基づいた分類を行った．しかし VirusTotal では各アンチウイルスソフトごとに検出結果に差異があり，必ずしも正しい結果になるとは限らない．そのため VirusTotal を用いたマルウェアの判定手法が課題としてあげられる．また本実験ではキャンペーンの分類方法として，subject および添付ファイル名の共通性を利用した．しかし実際には subject や添付ファイル名を変更させるスパムメールが存在する．そのため本文のコンテンツを分析し，キャンペーンの抽出精度を高めることが課題としてあげられる．

6 まとめ

本研究は，スパムトラップを用いてマルウェアが添付されたスパムメールの分析を行い，添付ファイルの種別ごとにマルウェアである確率などに差異があることを示した．スパムメールで送信されるマルウェアの多くはトロイの木馬型のウイルスであり，さらなるマルウエアの感染や情報の流出を目的としたものが多いことが確認できた．また添付ファイルとしては Zip ファイルや，Word 形式の文書ファイルなどが主に用いられていることが判明した．

参考文献

[1] Gianluca Stringhini, Oliver Hohlfeld, Christopher Kruegel, Giovanni Vigna, ‘’The harvester, the botmaster, and the spammer: on the relations between the different actors in the spam landscape”, 9th ACM symposium on Information, computer and communications security, 2014

[2] Christian Kreibich, Chris Kanich, Kirill Levchenko, Brandon Enright, Geoffrey M Volker, Vern Paxson, Stefan Savege “Spamcraft: An Inside Look At Spam Campaig Orchestration”,2nd USENIX conference on Large-scale exploits and emergent threats: botnets, spyware, worms, and more, Aug 2009.

[3] VirusTotal. https://www.virustotal.com/ja/

[4] Trend Micro, “MYDOOM”. http://about-threats.trendmicro.com/Malware.aspx?language=jp&name=MYDOOM

[5] Trend Micro, “「UPATRE」による攻撃とは”. http://about-threats.trendmicro.com/RelatedThreats.aspx?language=jp&name=Keeping+Up+with+the+Damage+of+UPATRE

[6] Trend Micro, “ボットネット「Zeus」 、「ZBOT」ファミリ、ボットネット「Kneber」の関係とは”. http://about-threats.trendmicro.com/RelatedThreats.aspx?language=jp&name=The+ZeuS\%2C+ZBOT\%2C+and+Kneber+Connection

[7] Microsoft Malware Protection Center, “Before you enable those macros…”. http://blogs.technet.com/b/mmpc/archive/2015/01/02/before-you-enable-those-macros.aspx