

# Sanesecurityのこと

小島 肇  
龍谷大学理工学部





## before

- FreeBSD + postfix 2.2 + amavisd-new + S25R
  - sophos (sophie) + clamav (clamd)



# amavisd-new

- MTA とコンテンツチェッカー（アンチウイルスやアンチスパム）とのインターフェイスとなるプログラム
  - 複数のアンチウイルスプログラムを併用できる
- amavisd-new が MIME を分解し、各パートをコンテンツチェッカーで検査する
- <http://www.ijs.si/software/amavisd/>



## E-card spam 襲来

- ある日、ウイルスサイトへのリンクが書かれたメールが大量に届き始めた
- それ自体はウイルスじゃないのでそのまま届く

アメリカ独立記念日に便乗するグリーティングカード - Mozilla Firefox

ファイル(F) 編集(E) 表示(V) 履歴(S) ブックマーク(B) ツール(T) ヘルプ(H)

http://www.sophos.co.jp/pressoffice/news/articles/2007/07

セキュリティ マスメディア アンチウイルス PC 情報 F1 SSH Cygwin Cisco Extreme iconv ねた

アメリカ独立記念日に便乗するグリーテ...

報道関係者向けガイド  
ニュースアーカイブ

プレスお問い合わせ

プレスお問い合わせ先

プレス資料

イメージ・ギャラリー  
ユーザー事例  
ホワイトペーパー  
所属業界団体

皆報フィード

セキュリティニュース  
会社情報

セキュリティニュース  
会社情報

皆報フィードとは？

2007年7月4日

アメリカ独立記念日に便乗するグリーティングカード

グリーティングカードを装い、猛威を振るうマルウェア？米独立記念日に便乗

ソフォスラボ (グローバルに展開するソフォスのウイルス・スパイウェア・スパム解析センター) のエキスパートは、7月4日のアメリカ合衆国の独立記念日に便乗し、一般ユーザーをトロイの木馬に感染させようとするハッカーからのスパムメールを警告しています。

このメールは、世界中のユーザーに送信され、友人からのグリーティングカードになりすまし、メール内のリンクをクリックさせようというものです。

Subject: America's 231st Birthday  
Date: 2007-07-03 14:26:12  
Body Size: 627

InfoButtons Paragraphs Images Preferences Send Corpora

Hi. Mate has sent you a greeting card.  
See your card as often as you wish during the next 15 days.

SEEING YOUR CARD

If your email software creates links to Web pages, click on your card's direct ww address below while you are connected to the Internet:

<http://www.dgreetings.com/2855a16e2a14205cd1712445ec8b2a44c6>

Or copy and paste it into your browser's "Location" box (where Internet addresses go).

PRIVACY  
dgreetings.Com honors your privacy. Our home page and Card Pick Up have links to our Privacy Policy.

TERMS OF USE  
By accessing your card you agree we have no liability.  
If you don't know the person sending the card or don't wish to see the card, please disregard this Announcement.

JavaScriptは禁止されています | <SCRIPT>: 3 | <OBJECT>: 0

完了

McAfee SiteAdvisor

<http://www.sophos.co.jp/pressoffice/news/articles/2007/07/july4.html>



2007.07.04 15:42:51 +0900

- 学内から学外へのメールが  
Email.Phishing.RB-1221 として検出された  
– 当時の e-card ねたの検出名
- その後も同様事例が数回発生
- なぜ学外→学内の時点で検出されなかったのか？



# 検出されたメールを分析

- メール本文にフィッシングメール全体(メールヘッダ+メール本文)が記載されているような転送メール
- ClamAV のフィッシング検出ルールはメールヘッダも見ているのか?



## after (phase 1)

- FreeBSD + postfix 2.3 以降 + amavisd-new + S25R
  - sophos (sophie) + clamav (clamd)
  - postfix milter interface + clamav-milter
  - 実際には postfix 2.4 を使用





# インストール

- /etc/mail/sendmail.mc に以下を追加
  - INPUT\_MAIL\_FILTER(`clmilter',  
`S=local:/var/run/clamav/clmilter.sock, F=,T=S:4m;R:4m')dnl  
define(`confINPUT\_MAIL\_FILTERS', `clmilter')
- cd /etc/mail; make install
- /etc/rc.conf に以下を追加
  - clamav\_milter\_enable="YES"  
clamav\_milter\_flags="-H -N -n -P --local --outgoing ¥  
--max-children=10 --quarantine-dir=/var/spool/quarantine ¥  
--external --timeout=0"



# インストール

- /var/spool/quarantine を作成
  - mkdir /var/spool/quarantine
  - chown clamav:clamav /var/spool/quarantine
  - chmod 700 /var/spool/quarantine
- /usr/local/etc/rc.d/clamav-milter.sh に以下を追加
  - start\_postcmd=start\_postcmd
  - start\_postcmd()
    - {
    - echo "5 sec waiting for \${clamav\_milter\_socket}..."
    - sleep 5
    - chgrp postfix \$clamav\_milter\_socket
    - chmod g+rwx \$clamav\_milter\_socket
    - }



# インストール

- `/usr/local/etc/postfix/main.cf` に以下を追加
  - `smtpd_milters = unix:/var/run/clamav/clmilter.sock`
  - `milter_default_action = accept`
- `/usr/local/etc/postfix/master.cf` に以下を追加
  - `127.0.0.1:10025 inet n - n - - smtpd`
  - `.....`
  - `-o smtpd_milters=`
- `clamav-milter` を起動し、`postfix reload`



## 結果

- ClamAV に対応されているものについては正常に検出されるようになった模様

しかし.....

8月にまたもや  
e-card spam  
大流行

悪意のあるグリーティングカードスパム、過去 48時間内に 900万通の配信 - Mozilla Firefox

ファイル(F) 編集(E) 表示(V) 履歴(S) ブックマーク(B) ツール(T) ヘルプ(H)

http://www.sophos.co.jp/pressoffice/news/articles/2007/08

セキュリティ マスメディア アンチウイルス PC 情報 F1 SSH Cygwin Cisco Extreme iconv ねた

悪意のあるグリーティングカードスパム、...

報道関係者向けガイド  
ニュースアーカイブ

プレスお問い合わせ

プレスお問い合わせ先

プレス資料  
イメージ・キャラクター  
ユーザー事例  
ホワイトペーパー  
所属業界団体

情報フィード  
セキュリティニュース  
会社情報  
セキュリティニュース  
会社情報  
情報フィードとは？

2007年8月16日

## 悪意のあるグリーティングカードスパム、過去 48時間内に 900万通の配信

ソフォス、グリーティングカードスパムをプロアクティブにブロック

ITセキュリティ・アンドコントロール大手のソフォスは、過去 48時間内に、900万通と推定されるグリーティングカードスパムが配信されていることを警告します。

ここ数週間に渡り、ソフォスは、受信者のコンピューターを感染させるよう仕組まれた Ecard スпамが復活したのを検知しています。ソフォスラボでは、過去 48時間の分析だけでも、JSEcard-A (英語) トロイの木馬を含むグリーティングカードスパムが、グローバルのスパムトラップで測定したスパム総数の 6.3%を占めていることを確認しています。

この一連のスパムには、ソーシャルエンジニアリング\*の手法が使われており、友人や親戚からのグリーティングカードを装います。メールには、メッセージに含まれているリンクを閲覧するだけで送られたグリーティングカードは、見ることができると記載されています。しかし、このリンク先をクリックすると得られるのは知人からの心温まるメッセージではなく、JSEcard トロイの木馬です。このトロイの木馬に感染してしまうと、コンピューターは更なる脅威にさらされることになります。

\*ソーシャルエンジニアリングとは、巧みな方法で機密情報を引き出す手段をいいます。

Sender IP: [redacted]

Cousin() has created Musical e-card for you at perfectgreetings.com.

To see your custom Musical e-card, simply click on the following Internet address (if your mail program doesn't support this feature you will need to COPY and PASTE the address into your browser's address box):

[http://\[redacted\]3933166b19e3393b5ca09ff74e82d](http://[redacted]3933166b19e3393b5ca09ff74e82d)

Send a FREE greeting card from [redacted] whenever you want by visiting us at: [redacted]

This service is provided and hosted by [redacted].

JavaScriptは禁止されています | <SCRIPT>: 3 | <OBJECT>: 0

完了

McAfee SiteAdvisor

http://www.sophos.co.jp/pressoffice/news/articles/2007/08/malicious-ecard.html



# spam 対策の重要性の増大

- ウイルス対策としての spam 対策が必要だと悟る
- しかし
  - 素の ClamAV の spam 対応は弱い
  - 金はない
  - 誤検出は困る



そこで.....


ClamAV - Unofficial Phishing Signatures - Mozilla Firefox

ファイル(F) 編集(E) 表示(V) 履歴(S) ブックマーク(B) ツール(T) ヘルプ(H)

http://www.sanesecurity.co.uk/

セキュリティ マスメディア アンチウイルス PC 情報 F1 SSH Cygwin Cisco Extreme iconv ねた

ClamAV - Unofficial Phishing Signa...



# Sanesecurity

... mad about email, sane about security ...

## Phishing and Scam Signatures for ClamAV

- Home
- News
- Blog
- Usage
- Downloads
- Statistics
- User Quotes
- Documents
- Thanks
- Feedback

[Clam AntiVirus](#) is a GPL anti-virus toolkit for UNIX and was coded to detect email viruses.

ClamAV's scanning engine is quite flexible and so has also been used to scan for phishing signatures. The Official phishing signatures in ClamAV are great but I've seen a number of phishing attempts get past the Official ClamAV signatures, so I thought I'd try to produce my own signatures to stop these phishing attempts (phish.ndb.gz).

I've also produced a small scam database (scam.ndb.gz) which will help detect some types of stock, lottery 419 and some image spams that are around at the moment. **Please read the Usage section before downloading.**

If you want to say thanks money-wise, feel free to donate something to charity here: [RNIB Online Donation](#) or [Cancer Research Online Donation](#)

Cheers,  
Steve

完了

McAfee SiteAdvisor

<http://www.sanesecurity.co.uk/>



# Sanesecurity

- ClamAV で利用できる、spam 検出用の独自のシグネチャを提供
- 無料
- ダウンロードするだけで利用できる



# ダウンロードスクリプト

ClamAV - Unofficial Phishing Signatures - Mozilla Firefox

ファイル(E) 編集(E) 表示(V) 履歴(S) ブックマーク(B) ツール(T) ヘルプ(H)

http://www.sanesecurity.co.uk/clamav/usage.htm

セキュリティ マスメディア アンチウイルス PC 情報 F1 SSH Cygwin Cisco Extreme iconv ねた

ClamAV - Unofficial Phishing Signa...

Linux (aka non-windows) Download Scripts (rename to .sh)		
Download	Author/Details	Last Updated
<a href="#">download script 1a</a>	Author: <a href="#">Norbert Buchmuller</a> : downloads the Phish and Scam databases. Also downloads the Third Party <a href="#">MSRBL</a> databases via Rsync (based on download script 1b) Note: this script will sleep for 30secs-10minutes in order to reduce strain on the server	26.09.07 <a href="#">UP</a>
<a href="#">download script 1b (old)</a>	Author: <a href="#">Rick Cooper</a> : downloads the Phish and Scam databases. Also downloads the Third Party <a href="#">MSRBL</a> databases via Rsync Note: this script will sleep for 30secs-10minutes in order to reduce strain on the server	14.08.07
<a href="#">download script 2</a>	Author: <a href="#">Bill Landry</a> : downloads the SaneSecurity Phish/Scam databases and the <a href="#">MSRBL</a> databases and <a href="#">SecuriteInfo</a> 's Unofficial malware database ( <a href="#">last version</a> )	25.09.07
<a href="#">download</a>	Author: <a href="#">Gerard Seibert</a> : downloads the Phish and Scam databases. Also downloads the Third Party	24.10.07

完了 McAfee SiteAdvisor

<http://www.sanesecurity.co.uk/clamav/usage.htm>



# ダウンロードスクリプト

- 複数のスクリプトが提供されている
  - Windows 用もある
- いずれにも MSRBL という RBL データのダウンロードが含まれている
  - 手元では、その部分はコメントアウトして利用



## after (phase 2)

- FreeBSD + postfix 2.3 以降 + amavisd-new + S25R
  - sophos (sophie) + clamav (clamd)
  - postfix milter interface + clamav-milter
  - Sanesecurity



# 使用感

- 英語圏の spam にはそれなりに有効
  - stock spam とか
- CJK spam にはめっぽう弱い
- 誤検出は確認していない

質問？