

クラウド・ホスティングサービスの迷惑メール対策

- ユーザーサイド・セキュリティ・インシデントの傾向
- クラウド・ホスティングサービスのインシデント検出方法と対策
- その他不正行為を目的としたサービス契約の流入阻止手法について



DAY

2017/10/5

COMPANY

さくらインターネット

DEPARTMENT

ネットセーフティ企画G

NAME

山下健一

さくらインターネット株式会社は
1996年にサービスを開始した、データセンターサービス、
ホスティングサービスプロバイダです。

- 従業員数 495名(2017年3月)
- 売上 139億(2017年3月・連結)



共有型ホスティングサービス

さくらのレンタルサーバ

- 共有型ウェブホスティングサービス
- 契約件数40万件突破（2016/7）
- 全プランPHP対応
- スタンダード以上はMySQL利用可能

人気No.1	ライト	スタンダード	プレミアム	ビジネス	ビジネスプロ
	広大なブログ、シンプルにホームページを運用したい方へ！	WordPress、EC-CUBE、独自SSL※対応の人気No.1プラン！※SNI SSL	動画や画像など多くのファイルを公開したい方へ！	複数人管理可能！サイトの運用・更新を外部委託しやすい法人向けプラン！	充実のセキュリティ！独自SSL対応でビジネスを強かにサポート！
	容量 10GB	容量 100GB	容量 200GB	容量 300GB	容量 500GB
	月額換算 129円 (年間料金 1,548円)	月額 515円	月額 1,543円	月額 2,571円	月額 4,628円

占有型ホスティングサービス

さくらのクラウド・VPS・専用サーバ

- OS自由インストール可能
- さくらのVPS 月額 ¥685円～
- 稼働IP総数 凡そ 10万IP前後位



abuse関連業務・数値

abuse 窓口対応数（2016年間）	数
メール受付対応数総計	約13000件
内・迷惑メール・フィッシング等	約4000件
内・セキュリティインシデント等	約4800件
内・権利侵害申立等	約3200件
内・その他法に反するもの等	約800件

- 1営業日換算 55件くらい
- 上記の他に書面对応/一部電話対応
訴訟/警察電話/捜査事項照会/差押令状対応など
- 増加傾向
- 窓口対応5人でがんばってます！

迷惑メールはどのように送信されるか・原因の種類と対策

セキュリティ・インシデント（ユーザーのサービスが悪用される）

- ウェブサイトやミドルウェアの脆弱性悪用・ファイルアップロード
- アカウント・パスワードクラック（SMTP, 各種CMS, Unixアカウント）
- どこから不正操作を実行するか

そもそも意図してやってる

- 詐欺・アドレス収集
「ねえ、**だよ、アドレス変わったから～」 「100万円受け取ってください」
- 不審な契約の流入阻止

セキュリティ・インシデント事例

- フィッシングサイトの検出履歴を調べてみる
- 典拠 PhishTank.com <https://www.phishtank.com/>
- さくらインターネット
AS7684, 9370, 9371, 2017/7～2017/8

※注

- 公開の検出情報を元にリスト作成 (成形しやすかった、という事情も)
- PhishTank.com では、2か月間に 19件 検出
- 同一サイトで複数URLを検出している場合は1件と算出
- 本例以外でもJPCERT/CC, SOC, NOC, セキュリティベンダー, 銀行, その他公的機関等からフィッシングサイト検出の連絡を受けています。
- PhishTank.com の履歴は情報源の一例
実際の被害数は数倍～

phish id	検出日	標的	フィッシングサイト URL	サイト構成
5195494	9月1日	bank of ireland	http://***.org/WordPress/wp-includes/images/boi/boi/authenticationdetails.htm	WordPress
5192887	8月31日	permanent tsb	http://***.org/WordPress/wp-includes/js/mediia.php	WordPress
5188326	8月29日	paypal	http://***.com/Welcome/2ce8669256114fc963b3f4bce5c0994c/?dispatch=***	WordPress
5179711	8月24日	BANRESERVAS	http://***.jp//NetBanking/Login.htm	WordPress
5162853	8月16日	paypal	http://***.com/file_upload/upload/dudsfac_files/account/hamed.php	WordPress
5156609	8月14日	Apple ID	http://***.net/wordpress/wp-content/plugins/easyrotator-for-wordpress/zipo/	WordPress
5150991	8月11日	twitter	http://***.xyz/pr/1/	故意に設置
5150713	8月11日	ebay	http://IP_Address/wordpress/wp-content/themes/Ad/index.php?bidderblocklogin&hc=***	WordPress
5143396	8月7日	alibaba.com	http://***.com/topics/sql/NewAli/	Dreamweaver
5132142	8月2日	paypal	http://***.jp/mp3/admin/Check_account/7874640798ABDS/Remove_limite_Acount_ppl/897946FDSREZ/Update_Your_Information/check-2017/mpp/	unknown
5129154	8月1日	dropbox	http://***.com/wp-includes/js/smw/db17/Home/	WordPress
5121681	7月27日	paypal	http://***.jp/upload_takanoko/upload/reikai/account/hamed.php	cgi uploader
5120061	7月27日	paypal	http://***.com/zing_post/upload/PopHopes2017/account/	cgi uploader
5116288	7月25日	alibaba.com	http://***.com/images/gram/alibaba/index.php?user=***	unknown
5109990	7月22日	paypal	http://***.net/config/Login/customer_center/customer-IDPP00C799/myaccount/signin/	unknown
5103579	7月18日	Chase bank	http://***.com/member/topics/files/****housing/joothersrd1.html	独自PHP
5095802	7月13日	unknown	http://***.jp:1080/yaatgrj5rxfl1ee7/aatgrj5rxfl1eei?id=F66A777EDD1D9431E4E06524C18D1500	Homepage Builder
5091613	7月11日	unknown	http://***.info/redirection_8copx1c/redirect/0n04mt-to-bt-internet	unknown
5085531	7月7日	unknown	http://***.com/de/sparkasse/login-online-banking.html=true/?sec=&token=	Homepage Builder

原因（推定）

PhishTank.com 2017/7～2017/8 の検出事例の場合の推定される原因

※ あくまで上記期間の検出公開情報を対象に原因推定するものであり、長期的傾向ではありません

CMSの管理の問題

- WordPress コアファイルの脆弱性・CMSをアップデートしていない
- 辞書攻撃

プロバイダ側の問題

- 故意の契約流入

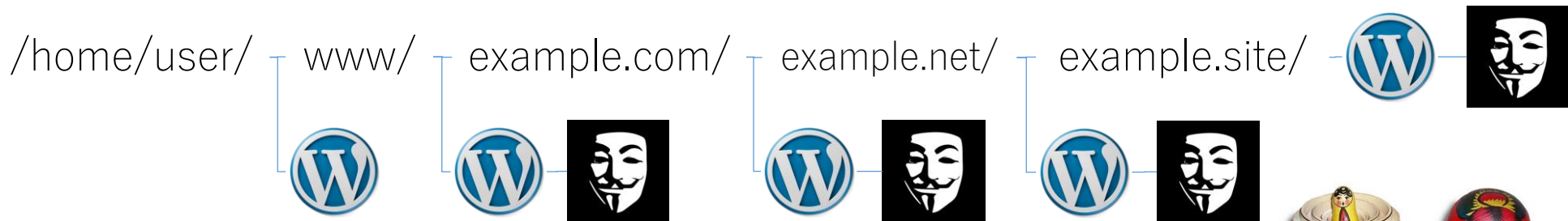
古典的CGIやPHPの問題

- アップロードを許可するファイルの拡張子制限が甘い
- ウェブサイトを更新管理していない

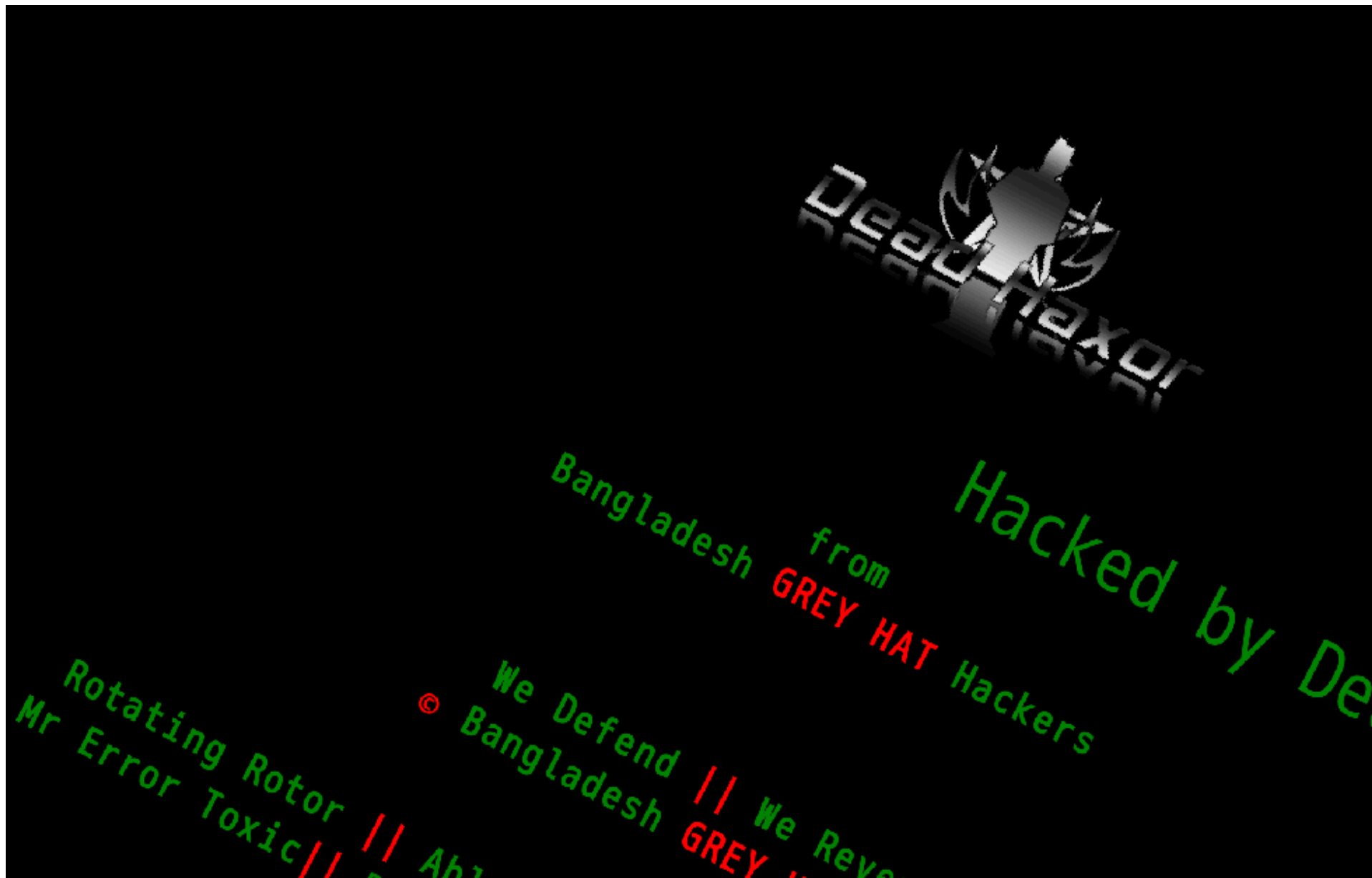
サイト管理用アカウントの問題

- 辞書攻撃？
- 怪しいプロキシが動作

- 攻撃者がファイルアップロード可能な場合、フィッシングキット以外にも様々なツールが利用される
- 設置されるツールの話
- そのツールを使うと何ができるかの話



- /home/user/www が改ざんされてるう
- /home/user/www/example.com が改ざんされてるう
- /home/user/www/example.com/example.net が改ざんされてるう
 - example.site/ も改ざんされてるう
- なんで /home/user 直下にもWordPressがあんねん！



```

Uname: FreeBSD [redacted].sakura.ne.jp 9.1-RELEASE-p24 FreeBSD 9.1-RELEASE-p24 #0: Thu Feb 5 10:03:29 JST 2015 root@ [redacted].sa [exploit-db.com]
User: 1065 ( [redacted] ) Group: 1000 ( users )
Php: 5.2.17 Safe mode: OFF [ ptpinfo ] Datetime: 2017-05-08 17:36:57
Hdd: 1983.69 GB Free: 1359.71 GB (68%)
Cwd: /home/[redacted]/www/ drwxr-xr-x [ home ]
    
```

Windows-1251

Server IP: 219.94.1[redacted]
Client IP: 210.165[redacted]

[Sec. Info] [Files] [Console] [Sql] [Php] [String tools] [Bruteforce] [Network] [Self remove]

File manager

Name	Size	Modify	Owner/Group	Permissions	Actions
[.]	dir	2017-05-08 02:06:12	/users	drwxr-xr-x	R T
[..]	dir	2017-04-25 20:00:19	/users	drwx---r-x	R T
[3d]	dir	2017-05-08 17:36:49	/users	drwx---r-x	R T
[all]	dir	2017-05-06 23:17:02	/users	drwxr-xr-x	R T
[amustone]	dir	2017-05-08 17:16:51	/users	drwx---r-x	R T
[appleart]	dir	2016-03-15 16:11:03	/users	drwx---r-x	R T
[[redacted]_blog_item]	dir	2013-06-07 16:16:24	/users	drwxr-xr-x	R T
[arstnews]	dir	2010-07-08 16:52:31	/users	drwxr-xr-x	R T
[banner]	dir	2011-11-02 20:43:40	/users	drwxr-xr-x	R T
[basic_authentication]	dir	2013-08-27 10:53:04	/users	drwxr-xr-x	R T
[cad]	dir	2017-05-01 01:32:57	/users	drwxr-xr-x	R T
[config]	dir	2017-04-25 21:15:47	/users	drwxr-xr-x	R T
[contra]	dir	2013-02-23 16:57:41	/users	drwxr-xr-x	R T
[css]	dir	2006-10-23 16:59:04	/users	drwxr-xr-x	R T
[css-sen]	dir	2009-07-19 17:10:19	/users	drwxr-xr-x	R T
[css2]	dir	2006-10-23 16:59:01	/users	drwxr-xr-x	R T
[data]	dir	2017-05-08 06:13:58	/users	drwx---r-x	R T
[dtm]	dir	2017-04-25 14:13:06	/users	drwx---r-x	R T
[EN]	dir	2017-05-05 05:09:24	/users	drwxr-xr-x	R T
[fb]	dir	2014-05-16 18:00:18	/users	drwxr-xr-x	R T
[fm]	dir	2009-11-21 17:29:14	/users	drwxr-xr-x	R T
[fm-new]	dir	2014-02-08 14:22:32	/users	drwxr-xr-x	R T
[fm2]	dir	2017-01-28 17:04:54	/users	drwx---r-x	R T
[harada]	dir	2014-07-15 19:42:13	/users	drwxr-xr-x	R T
[img]	dir	2013-02-20 14:19:14	/users	drwxr-xr-x	R T
[img-f]	dir	2017-02-20 14:19:57	/users	drwxr-xr-x	R T

“WebShell” をGoogle検索

Deprecated: Function ereg_replace() is deprecated in /home/7public_html/fikeu.php(6) :eval()'d code on line 1

1337w0rm

PHP, INI CRACKER

User :

Pass :

Type : Simple : /etc/passwd :

start

CMD MYSQL

user pass database

cmd ~

```
SHOW DATABASES;
SHOW TABLES user_vb ;
SELECT * FROM user;
SELECT version();
SELECT user();
```

run

“1337w0rm” をGoogle検索

Leaf PHPMailer 2.7

Email

Sender Name

Attachment (Multiple Available)

No file selected

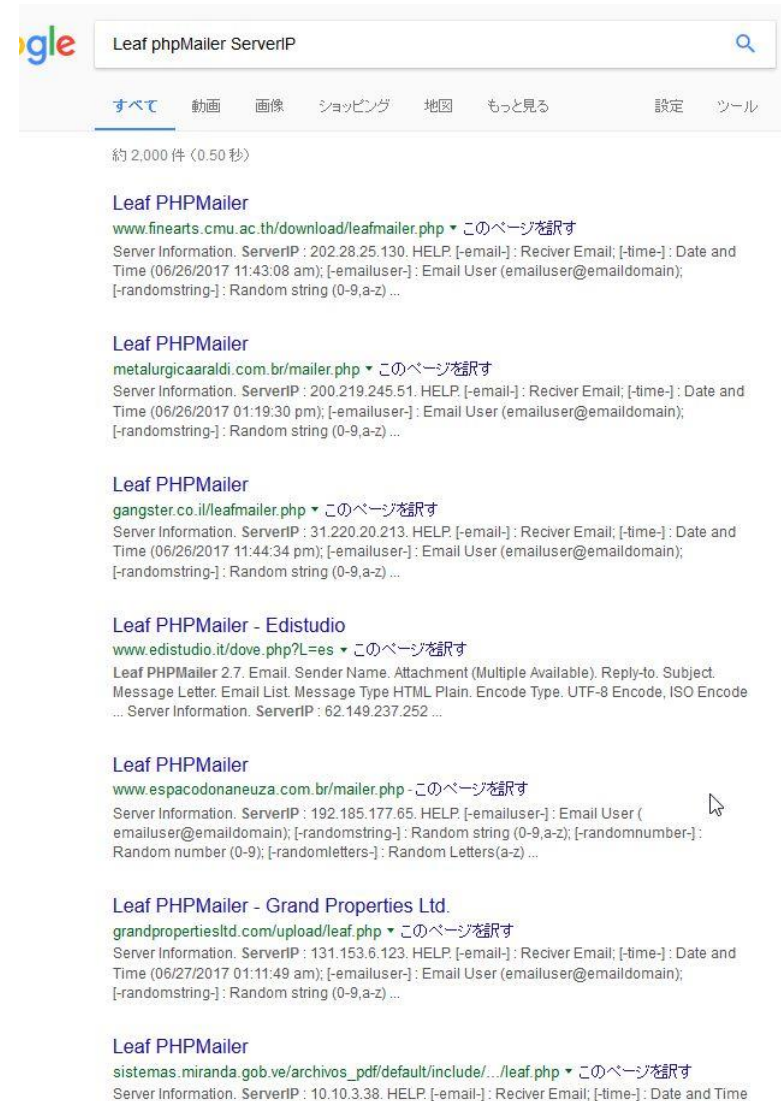
Reply-to

Subject

Message Letter

ウェブサイトのインシデントで起こること

- 示威行為
 - “Hacked by ****” と書く、書いた画像を置く
 - 同時に何が行われたかにより深刻度が変わる
- WebShell, バックドアを設置
 - 外形からは見つけにくい
認証・接続元IP制限・検索エンジンブロック等
 - ファイルアップロード、ファイル改ざん
 - プロキシ、bot, DoS, bruteforce攻撃ツール を設置
次のVICTIMを捜索
- データベース接続アカウントのクラック試行
- マルウェアサイトURLを埋め込む、
リダイレクトする
- メール送信ツールを設置
 - Leaf PHP Mailer 他 PHP Mailer 等をググると楽しい
 - あちこち変なブツ置かれてオカシな事になっている
 - フィッシングサイト = 蟻地獄・待ち受け型
同時にどこかでフィッシングメールが送信される
- とにかく色々変なツールが置かれて！！



Leaf phpMailer ServerIP

すべて 動画 画像 ショッピング 地図 もっと見る 設定 ツール

約 2,000 件 (0.50 秒)

Leaf PHPMailer
www.finearts.cmu.ac.th/download/leafmailer.php ▾ このページを訳す
Server Information. ServerIP : 202.28.25.130. HELP. [-email-]: Reciver Email; [-time-]: Date and Time (06/26/2017 11:43:08 am); [-emailuser-]: Email User (emailuser@emaildomain); [-randomstring-]: Random string (0-9,a-z) ...

Leaf PHPMailer
metalurgicaaraldi.com.br/mailler.php ▾ このページを訳す
Server Information. ServerIP : 200.219.245.51. HELP. [-email-]: Reciver Email; [-time-]: Date and Time (06/26/2017 01:19:30 pm); [-emailuser-]: Email User (emailuser@emaildomain); [-randomstring-]: Random string (0-9,a-z) ...

Leaf PHPMailer
gangster.co.il/leafmailer.php ▾ このページを訳す
Server Information. ServerIP : 31.220.20.213. HELP. [-email-]: Reciver Email; [-time-]: Date and Time (06/26/2017 11:44:34 pm); [-emailuser-]: Email User (emailuser@emaildomain); [-randomstring-]: Random string (0-9,a-z) ...

Leaf PHPMailer - Edistudio
www.edistudio.it/dove.php?L=es ▾ このページを訳す
Leaf PHPMailer 2.7. Email. Sender Name. Attachment (Multiple Available). Reply-to. Subject. Message Letter. Email List. Message Type HTML Plain. Encode Type. UTF-8 Encode, ISO Encode ... Server Information. ServerIP : 62.149.237.252 ...

Leaf PHPMailer
www.espacodonaneuza.com.br/mailler.php - このページを訳す
Server Information. ServerIP : 192.185.177.65. HELP. [-emailuser-]: Email User (emailuser@emaildomain); [-randomstring-]: Random string (0-9,a-z); [-randomnumber-]: Random number (0-9); [-randomletters-]: Random Letters(a-z) ...

Leaf PHPMailer - Grand Properties Ltd.
grandpropertiesltd.com/upload/leaf.php ▾ このページを訳す
Server Information. ServerIP : 131.153.6.123. HELP. [-email-]: Reciver Email; [-time-]: Date and Time (06/27/2017 01:11:49 am); [-emailuser-]: Email User (emailuser@emaildomain); [-randomstring-]: Random string (0-9,a-z) ...

Leaf PHPMailer
sistemas.miranda.gov.br/archivos_pdf/default/include/.../leaf.php ▾ このページを訳す
Server Information. ServerIP : 10.10.3.38. HELP. [-email-]: Reciver Email; [-time-]: Date and Time

WordPressプラグイン Welcart 脆弱性の悪用

- オブジェクトインジェクションの脆弱性
ver 1.9.3 以前のすべてのバージョン対象
- 2017/9/13 修正バージョン ver1.9.4 リリース
- 2017/9/8 時点でカーニバル状態

「CMSを使用する」ことの難しさ

- メジャーなCMSはどうしても狙われる
- 自動アップデートの重要性・wp-cron.php の限界
- CMSを使用する場合でも「HTMLソースを読む知識」は必要

基本的な対策手法・検出手法（主に「さくらのレンタルサーバ」の場合）

- サービス設計における対策
 - 単位時間あたりに送信可能なメール通数上限をサービスプランごとに設定
 - 外部レジストラ登録ドメインの持ち込み制限（お試し利用時）
 - 日本国外IPからのSMTP認証をデフォルト拒否
- 事後対応・外部DNSBLの登録状況をモニターし登録時に調査
 - SPAMHOUSE SBL, BarracudaCentral, SORBS
 - 今後調べたいもの、モニター効果確認中のもの
nix_spam, uceprotect.net, backscatterer.org

異常が確認された場合の対応

- 異常が認められたウェブページの上位ディレクトリのパーミッションを落とす
- SMTPの認証記録調査・異常な数の認証成功があればパスワード強制変更
- ユーザーへの連絡

リスクを簡潔に説明して何とかする

この度、ご利用中のサービス「●●●●」より、不審なメールが送信されているとの通報が弊社へ寄せられました。

第三者により、迷惑メールやフィッシングメール等を送信する踏み台に悪用されている可能性が考えられるため、至急、調査と対策を実施いただけますようお願いいたします。

本件に関しましては、ご対応結果について、201*/**/**までに本メール返信にてご連絡いただきますようお願いいたします。

上記の期限までにご連絡がない場合、または継続して通報が寄せられる場合には、被害拡大防止の為、ご利用サービスの一時停止などの緊急措置を行わせていただくことがございますので、予めご了承ください。

○考えられる原因（略）

○必要な対策（略）

■注意事項・考えられるリスク

- 対策が不十分な場合、再発する危険があります。
- お客様のウェブサイトが改ざんされ、ウイルスを配布している可能性があります。
- **ウェブサイトを読覧したご家族・ご友人・職場・取引先・その他のコンピュータにウイルス感染の被害を引き起こした可能性があります。**
- フィッシングメールや標的型攻撃メールを送信した可能性があります。
- **ウイルス感染や情報漏えいの被害を引き起こした可能性があります。**
- 悪意を持って設置されたファイルを全て削除することは困難です。
- **完全な再発防止のためには、サーバ内の全てのファイルを削除することをお勧めします。**

※ユーザーに送る連絡メールの一例

予防策

- 強固なパスワードを設定する
 - ファイアウォールを設定する
 - 自動アップデートを利用する
 - 定期的にバックアップを取る
- 耳タコのこの4つ、「徹底」するのは実はかなり難しい
 - 担当者の不在・担当者が変わる・部署移動・組織変更
 - キャンペーンサイト・保守方針や運用期間があいまいなサイト
 - 或いは
 - パスワードを一切使用しない（現実的には無理）
 - インターネットに接続しない（現実的には無理）
 - バグを出さない（現実的には無理）
 - プラグインの脆弱性は修正リリース前に攻撃を受ける例も完全予防困難？

セキュリティインシデント警戒・早期検出手法

- 外部のブラックリスト・ブロックリスト類をモニターする早期警戒の話
- 各ブロックリストの検出感度・信頼性を評価する方法

ProjectHoneyPot (<https://www.projecthoneypot.org/>)

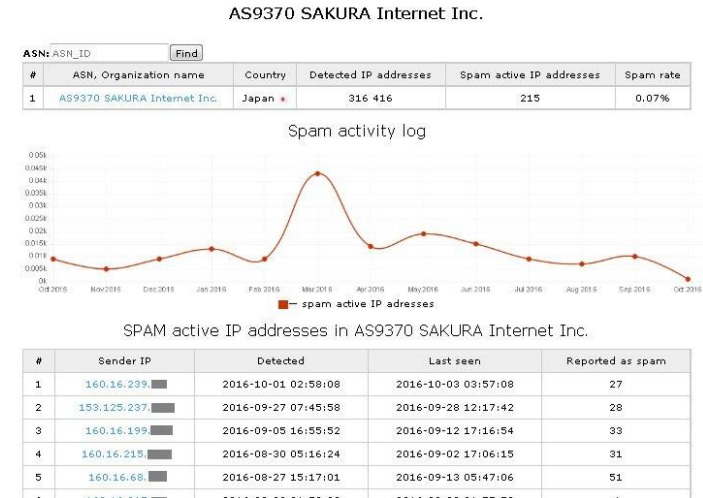
```
# mail.example.com (192.168.1.3)
$ dig +short ${API_KEY}.3.1.168.192.dnsbl.httpbl.org
127.1.20.1
```

- API Key を取得することで DNS問い合わせコマンドを用い SPAM検出を問い合わせ可能
 - 多数のIPを一気に問い合わせることができる
- 第二オクテットは最新SPAM検出後経過日数
 - 最新検出日情報がわかることが重要
- http://www.projecthoneypot.org/ip_192.168.1.3 形式のURLで SPAM検出の詳細情報を閲覧可能
メール件名が掲載されているので便利
- 迷惑メールか、フィッシングメールか
 - 件名で推測
 - フィッシングメールならばフィッシングサイトも設置されている可能性が大

The screenshot shows the Project Honey Pot website interface. At the top, there's a navigation bar with links for Home, IP Data, Statistics, Services, Help, and About. Below this is a sub-navigation bar with links for Directory of IPs, Lookup IP, Harvesters, Spam Servers, Dictionary Attackers, and Comment Spammers. The main content area is titled "IP Address Inspector" and displays information for the IP address 49.212.142.100. A warning message states: "Please note: being listed on these pages does not necessarily mean an IP address, domain name, or any other information is owned by a spammer. For example, it may have been hijacked from its true owner and used by a spammer." Below this, there's a "Look up IP in:" section with links to Domain Tools, SpamHaus, Spamcop, SenderBase, Google Groups, and Google. The "Geographic Location" is identified as Japan. A table shows: "First Received From" approximately 3 weeks ago, "Last Received From" within 1 week, and "Number Received" 22 email(s) sent from this IP. At the bottom, it shows "Dictionary Attacks" 6 email(s) sent from this IP. There is also a link for "Top Mail Server List".

CleanTalk (<https://cleantalk.org/blacklists/AS9370>)

- ウェブサイトのコメントスパム対策
- 幅広いCMSに対応
特にWordPress に対応しているために利用者が多い
- ブロック日時・履歴を公開
- プロキシ・中華VPN・不正アクセス発信の検出効果



Blocklist.de (<https://www.blocklist.de/en/search.html?as=9370>)

- “fail2ban” がbanした通信元IPアドレスをブラックリスト化して公開
- 不正アクセス・bruteforce 発信の検出効果
- 検出サイト・サーバはクラックされている



Fail2Ban でできる事

- ログから認証失敗記録等を監視
設定した回数認証失敗した場合に iptables 等で遮断
- http access_log 類も監視可能、
各種インジェクションコマンド類も設定次第で遮断可能
- 遮断時、blocklist.de, badips.com, dshield.org に
レポートする機能を同梱
- 簡易IDS
遮断発動時、指定したアドレス宛にメール通知

sendmail.conf を弄って、通知先を IP管理事業者に向ける人が居る

- 連絡先情報確認にabusix <https://www.abusix.com/contactdb> を
使用する例が多い
(whoisやrdapを直接使って欲しいが…やはりDNSが速い)
- 攻撃者に攻撃用の踏み台を入手させないことが重要
通知が得られれば事業者は対応ができる

```
[root@centos7]# yum install epel
[root@centos7]# yum install firewalld fail2ban
[root@centos7]# systemctl start firewalld
[root@centos7]# systemctl enable firewalld
[root@centos7]# cp /etc/fail2ban/jail.conf,.local
[root@centos7]# vi /etc/fail2ban/jail.local
[root@www fail2ban]# diff -u /etc/fail2ban/jail[.conf,.local]
--- jail.conf
+++ jail.local
@@ -226,6 +226,7 @@
 port    = ssh
 logpath = %(sshd_log)s
 backend = %(sshd_backend)s
+enabled = yes

[root@centos7]# systemctl start fail2ban
[root@centos7]# systemctl enable fail2ban
```

```
[root@www fail2ban]# ls /etc/fail2ban/action.d/*.conf
/etc/fail2ban/action.d/badips.conf
/etc/fail2ban/action.d/blocklist_de.conf
/etc/fail2ban/action.d/dshield.conf
/etc/fail2ban/action.d/sendmail.conf
```

```
$ dig www.sakura.ad.jp +short
163.43.24.70
$ dig 70.24.43.163.abuse-contacts.abusix.org txt +short
"hostmaster@nic.ad.jp"
```


FireHOL IP Lists (<http://iplists.firehol.org/>)

- iptables + ipsetを補助するOSS
 - ipset を使えば数万単位に及ぶ多数のIPをハッシュ化してiptablesに取り込める
- いろんなブロックリスト横断収集してgitに公開
- CleanTalkもStopForumSpamもBlocklist.deもTor node もbitcoin nodes も botscout も、ほしい物は大概なんでもある
 - 多様なリストが網羅されている
- IPアドレス記載形式が ipset コマンド用に統一されている、あまりにも便利で涙が出る
 - 形式が統一されている
- どのリストが役に立つかは地道な評価が必要、でもこれで勝つる！ かもしれない！
- update-ipsets コマンドでリストを一気にぶっこぬく、サービス運用IPと照合

The screenshot shows the FireHOL IP Lists website interface. At the top, there are navigation tabs: "FireHOL IP Lists", "Home", and "Evolution". Below the navigation, there's a search bar with "Found a bug?" and "Search issues". The main content area is titled "All IP lists monitored" and has three filter tabs: "By Category", "By Maintainer", and "Alphabetically".

The "abuse" category is selected, showing a list of IP lists with their respective update frequencies. The list includes items like "blocklist_net_ua", "botscout", "cleantalk", "firehol_abusers_1d", "gpf_comics", "ipblacklistcloud_recent", "myip", "stopforumspam", etc. Each item has a colored label indicating its update frequency (e.g., "now", "this hour", "this week", "today", "4 hours", "older").

To the right of the list is a bar chart titled "Number of Unique IPs". The y-axis ranges from -50,000 to 300,000,000. The chart shows a single bar for the "abuse" category, which is very tall, reaching approximately 300,000,000. Below the chart, there's a caption: "The chart below shows the update. Using the chart below we a" followed by a bullet point: "• How much of this IP I".

At the bottom right, there's a section titled "Country Map" with a sub-caption: "Each time an ipset is updat IP2Location.com Lite count Using the maps below we a" followed by two bullet points: "• Which countries doe" and "• Where do the attack".

事業者として公開ブロックリストを評価するポイント

• 揮発性

- どんどん消えていく情報が良い
- 古い情報（既に削除済み・対応済みなど）はリストのノイズにしかない

• 感度

- 感度が高い＝検出する、感度が低い＝検出しない

• 照合速度

- リスト化されている・DNSで問合せできるものは照合速度が速い
- 1IPアドレス単位でHTTPクエリを投げて調べる必要があるものは役に立たない

• 検出の事実と時期が公開されているか

- 非公開情報は役に立たない・公開されていることが重要
非公開情報はユーザーへの通知に使用できない
- 検出した日付が不明のモノはユーザーへの通知にふさわしくない

• 検出の機序が公開されているか

- なぜ検出できたのかがわからないと困る
(通信の秘密の侵害・スキャン・不正アクセスしていると疑われる可能性)
- 正報・誤報を判断する情報

評価は大変・非常に時間がかかる

- 公開リスト毎に揮発性・感度・速度・利便性・信頼性の優劣があり見極めに時間がかかる
- 劣るリストにもセカンドオピニオンの価値はある
(優れるリストであっても、いち通信事業者がリスト運営団体の信頼性を保証できる訳ではない)

通信事業者の立場だからこそ、できること

- 多数のIP・サイトを運用しているから、リストの有効性 (+有効性の変化・トレンド) を評価できる
- 多数のIP・サイトを運用しているから、リストをモニターし対応効果が得られる
- なんの情報も欠けているか・継続的な情報収集の必要性も判断できるだろう

優れる	劣る	劣る理由
(無)	PhishTank.com	感度が今一つ
ProjectHoneyPot.org	SPAMHOUSE SBL 他・DNSBL類	検出日が不明・速度が遅い
CleanTalk.org	StopForumSpam.com	感度が低い
Blocklist.de	BadIPs.com, AbuseIPdb.com	感度・速度が低い
ShadowServerFoundation (非公開で使いにくい)	CleanMX, VirusTotal, Malware Domain List, Malc0de, Zeustracker, CBL&XBL	揮発性が最低・正誤判定困難 (DNS Sink Hole の情報が欲しい)
(Google検索が最速)	Proxylists.net	感度が今一つ

公開ブロックリストを使用するメリット

- 一般システム管理者にとってのメリット（本来用途）
- 通信事業者にとってのメリット・通信の秘密を順守する観点
- 多数のIPを運用する事業者だからこそそのメリット・ユーザーのメリット

公開ブロックリストからわかること

さくらインターネットがヤバいのか？ 他のIPはどうなのか？

- 公開ブロックリスト記載IPをgeoip等でASN照合
- 国別・事業者別（ISPか・ホスティングか）・検出内容の分布を調べる
- 不正アクセスの検出はわりとあっちこっちに
- 宅内・事務所内・http/https ポートフォワード先の保守していないNASとかどうもヤバそうな雰囲気
- 他にもわかること・・・

不審な契約の流入阻止について

スパマーの契約手口

- いつ、契約手続きするか
- どういうツールを使用して迷惑メールを送信するか

対策の方法

- 入金前の制限
外部登録ドメインの持ち込み制限・OP25B
- 契約時の登録電話番号実在検証・音声/SMS認証
- 書面による住所確認

効果・悩み・今後の方向性

最後に

- 事業者としてできること
セキュリティ・インシデント、異常なメール送信警戒
- 警戒しつつも、問題検出には限界
外部からの苦情通報が重要
- さくらインターネット「abuse問合せフォーム」
<https://secure.sakura.ad.jp/form/abuse.php>

ご清聴ありがとうございました。