Dionaeaでハニーポットを作ってみた話

越後ネットワーク・オペレーターズ・グループ (ENOG)

江部 仁士

自己紹介

- 名前
  - ✓ 江部　仁士
- 仕事
  - ✓ネットワークやサーバの構築、運用
- 参加コミュニティ
  - ✓ ENOG

お話の流れ

- ENOGのご紹介
- ハニーポットのお話
- 受けた攻撃のお話

ENOGのご紹介

- **ENOGとは**
  - ✓ **E**chigo **N**etwork **O**perators' **G**roup
  - ✓ 新潟県内を拠点とした地域NOG
  - ✓ http://enog.jp/

Ai Echigoya
ENOG公認キャラクタ

ENOGのご紹介

- **主な活動内容**
  - ✓ Enog Meeting　＜　勉強会 & 懇親会　＞
    - ➢ 2ヶ月に1度開催 (昨日で34回目)
    - ➢ 誰でもWell Come!　LT大歓迎!

ハニーポットのお話

ハニーポットとは

- 不正アクセスを受けることに価値を持つシステム

By Wikipedia

ハニーポットの種類

- **高対話型ハニーポット**
  - ✓ 脆弱性を残した「本物」のOSやアプリケーションなどをハニーポットとして利用する
  - ✓ 高度な情報を得ることができる
  - ✓ 侵入されたときのリスクが高い

- **低対話型ハニーポット**
  - ✓ OSやアプリケーションの動作をエミュレート
  - ✓ 比較的安全に運用できる
  - ✓ 機能が制限されているため、情報量は落ちる
  - ✓ スキャンで検出される可能性あり

ハニーポットの選定

- 2012年11月20日に欧州ネットワーク情報セキュリティ庁から発行された資料のハニーポットの評価結果

NAME	DETECTION SCOPE	ACCURACY OF EMULATION	QUALITY OF COLLECTED DATA	SCALABILITY AND PERFORMANCE	RELIABILITY	EXTENSIBILITY	EASE OF USE AND SETTING UP	EMBEDDABILITY	SUPPORT	COST	USEFULNESS FOR CERT
LOW-INTERACTION SERVER-SIDE HONEYPOTS											
General purpose honeypots											
Amun	MULTI	★★	★★★	★★★	★★★★	★★★★	★★★	★★★	★	$	
Dionaea	MULTI	★★★	★★★★	★★★	★★★★	★★★★	★★★	★★★★	★★★★	$	
KFsensor	MULTI	★★	★★★	★★★★	★★★★	★★★	★★★★	★★★	★★★	$$	
Honeyd	MULTI	★★	★	★★★★	★★★★	★★★★	★★★	★★	★	$	
Honeytrap	MULTI	★★	★★	★★★★	★★★	★★★	★★	★	★★	$$	
Nepenthes	MULTI	★★	★★	★★★	★★★★	★★★★	★★★	★★	★	$$	
Tiny Honeypot	MULTI	★★★	★★	★★★	★★★★	★★★★	★★	★★	★	$$	
Web application honeypots											
DShield Web Honeypot	SPEC	★★	★★	★★★	★★★★	★★★	★★★	★★	★★	$$	
Google Hack Honeypot	SPEC	★★	★★★	★★★★	★★★	★★★★	★★★	★★★	★	$	
Glastopf	SPEC	★★★★	★★★	★★	★★★	★★★★	★★★	★★★	★★★★	$	
SSH Honeypots											
Kippo	SPEC	★★★	★★★	★★	★★★	★★	★★★	★★	★★★	$$	
Kojoney	SPEC	★★★	★★	★★★	★★	★★	★★	★★	★	$$$	
SCADA Honeypots											
SCADA HoneyNet Project	MULTI	★★	★	★★★	★★★	★★	★★	★★★	★	$	
SCADA HoneyNet (Digital Bond)	MULTI	★★	★	★	★★	★★	★★	★	★	$$	
VoIP Honeypots											
Artemisa	SPEC	★★★★	★★★★	★★	★★★	★★	★★★	★★	★	$$	
Bluetooth Honeypots											
Bluepot	SPEC	★★★	★★	★★★	★★	★★	★★★	★	★	$$$	
Sinkholes											
HoneySink	MULTI	★★★	★★★★	★★★	★★★★	★★	★★	★★★	★	$$	
USB Honeypots											
Ghost USB honeypot	SPEC	★★★	★★	N/A	★★★	★★	★★★	★★★★	★★	$$$	

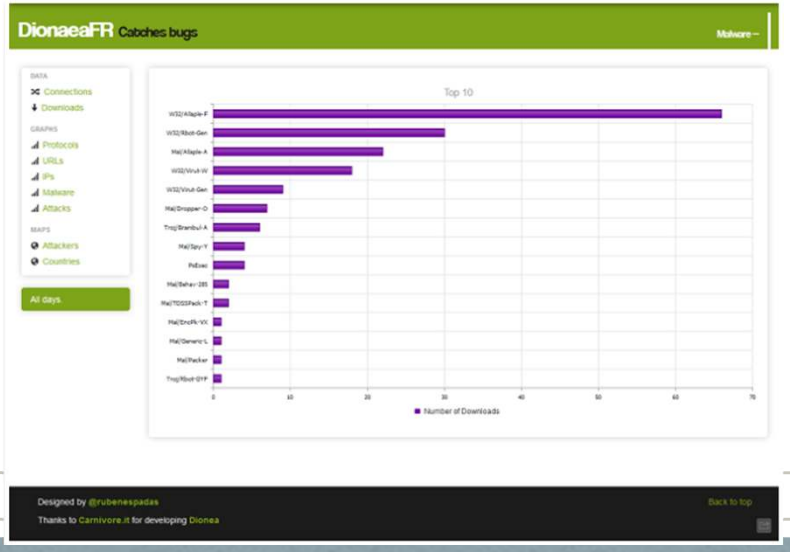
Proactive Detection of Security Incidents- Honeypotsより

Dionaea(ハエトリグサ)

- **Nepenthes(ウツボカズラ) の後継**
- **低対話型ハニーポット**
  - ✓マルウェア収集向け
- **提供サービス**
  - ✓SMB , HTTP , HTTPS , FTP , TFTP , MSSQL , MySQL , SIP
- **IPv6対応、TLS対応**

Dionaea(ハエトリグサ)

- **Virus Totalとの連携**
  - ✓Virus Totalでアカウント登録しPublic API Keyを入手する必要あり
- **ログ解析ツール**
  - ✓DionaeaFR

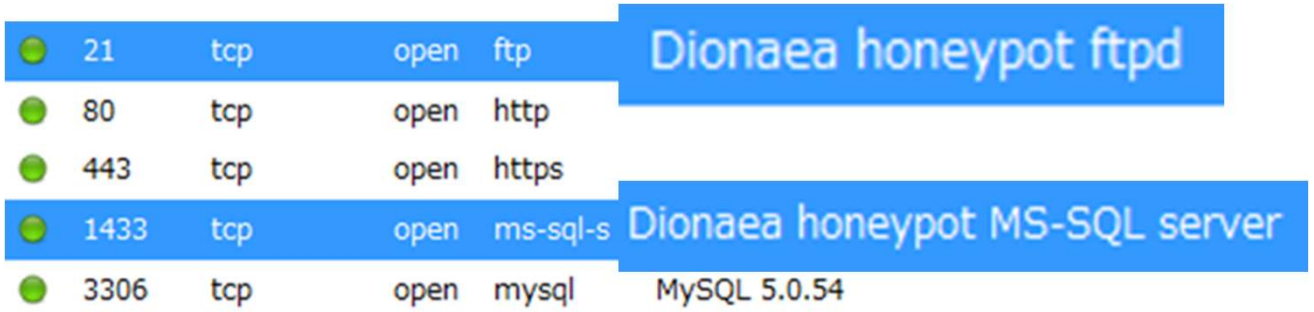


公開前にやっておくこと

- **セキュリティ対策**
  - ✓OSやアプリケーションに脆弱性を残さない
  - ✓リモートアクセスは許すな
    - ✓アクセス制限
    - ✓鍵認証

公開前にやっておくこと

- **nmap対策**
  - ✓ハニーポット特有の挙動を示すシグネチャを保持



  - ✓nmapのシグネチャ
    - ✓ https://svn.nmap.org/nmap/nmap-service-probes

公開前にやっておくこと

- **ログ管理**
  - ✓デフォルトではdebugレベルのログを収集
  - ✓1日で数十ＧＢのログが溜まることも。。。
  - ✓設定でログレベルを下げてログの量を減らす

/opt/dionaea/etc/dionaea.conf

```
logging = {
        default = {
                file = "log/dionaea.log"
                levels = "all"
                domains = "*"
        }

        errors = {
                file = "log/dionaea-errors.log"
                levels = "warning,error"
                domains = "*"
        }
    }
```

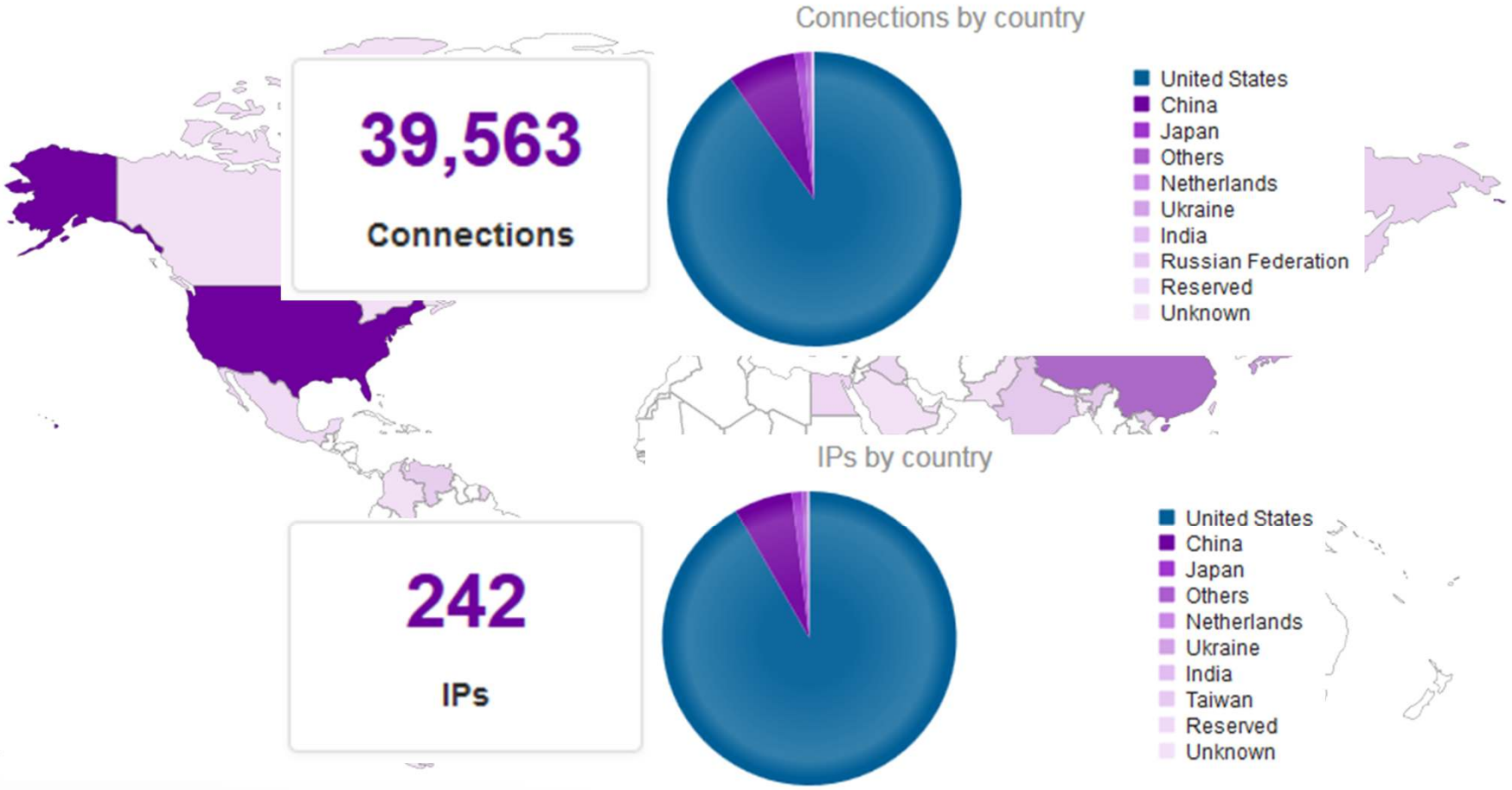
levels = “all,-debug”に変更

levels = “error”に変更

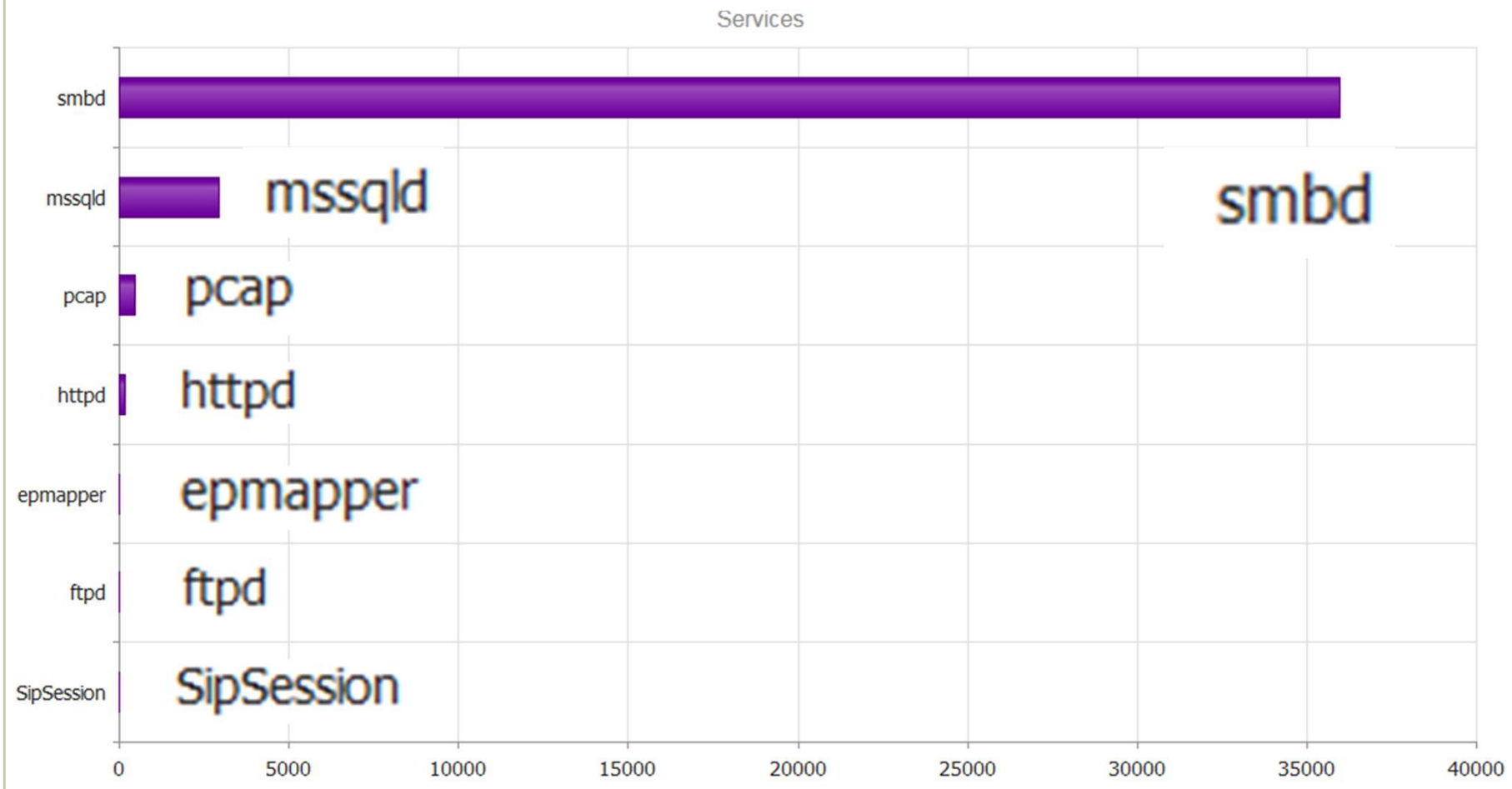
受けた攻撃のお話

不正アクセス数

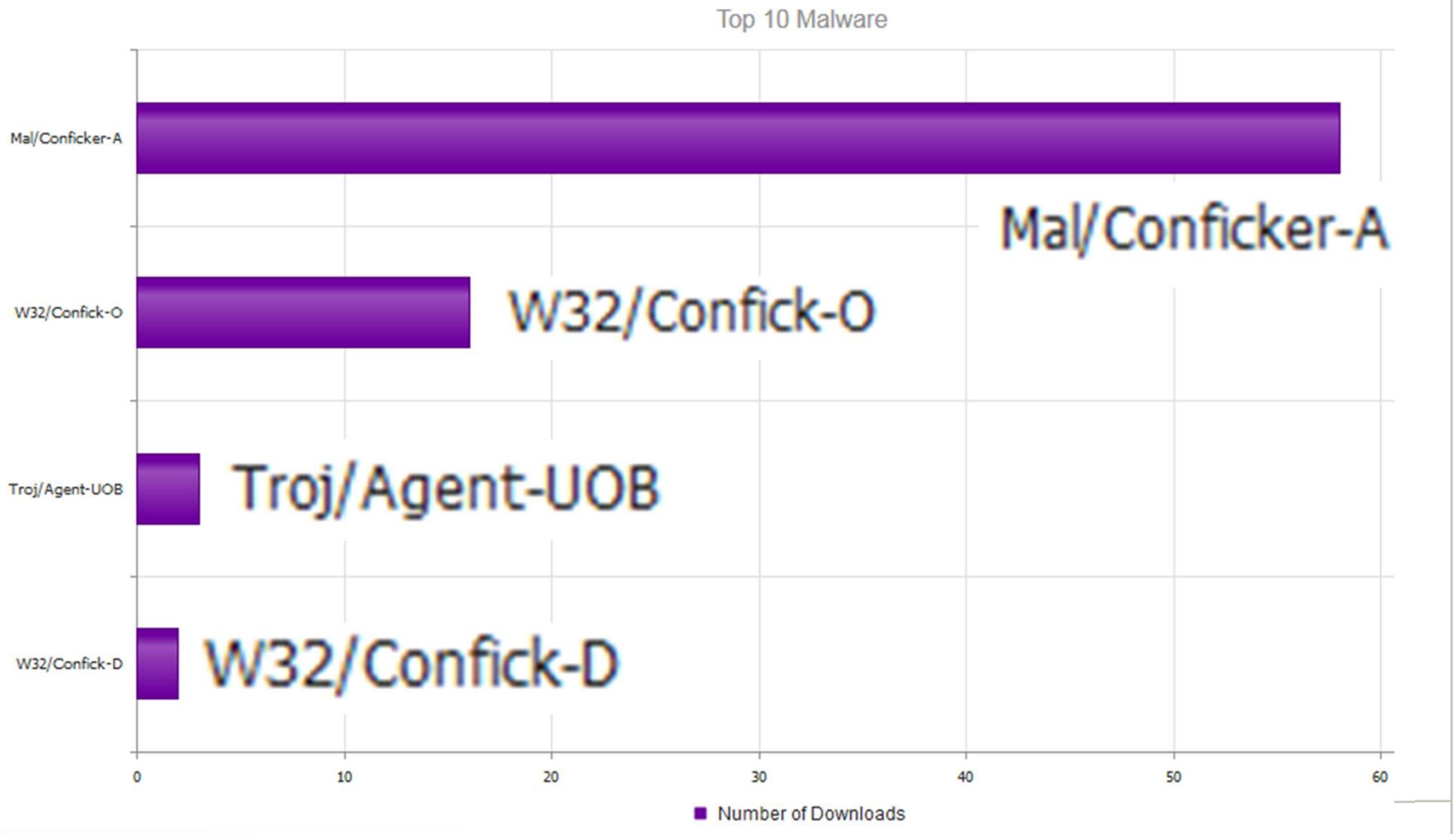
- **集計期間：　2週間**



サービス毎のアクセス数



入手したマルウエア


Top 10 Malware
Mal/Conficker-A
W32/Confick-O
Troj/Agent-UOB
W32/Confick-D
Mal/Conficker-A
W32/Confick-O
Troj/Agent-UOB
W32/Confick-D
0
10
20
30
40
50
60
Number of Downloads

ShellShock問題

- 昨年9月に発見されたBashの脆弱性
  - ✓CVE-2014 1 -6271、CVE-2014-7169
- CGI経由でOSコマンドの実行が可能

ShellShock問題

1．CGIへのアクセス
　　以下の不振なPerlのコード

2．XSUCCESSの表示

3. System関数でOSコマンドの実行

定番の不正アクセス

- **EPGrec**
  - ✓ GET /epgrec/templates/envSetting.html HTTP/1.1
  - ✓ EPGrecはWebベースの録画予約システム
- **phpMyAdmin**
  - ✓ GET /phpmyadmin/scripts/setup.php HTTP/1.0
- **WordPress**
  - ✓ GET /wp-login.php HTTP/1.0
  - ✓ GET /xmlrpc.php HTTP/1.0

最後に

- **サイバー攻撃は日常茶飯事！**

- **最新セキュリティ情報をチェック**
  - ✓ 情報セキュリティサイトのRSS、MLを活用
    - ✓ JPCERT/CC , IPA

- **定期的なセキュリティチェック**
  - ✓ 脆弱性スキャンツール
    - ✓ OWASP ZAP、skipfish、Open VAS…etc

Fin

ご清聴ありがとうございました