複数拠点のハニーポットを活用した新たな脅威の検出と分析手法の共有

株式会社ラック サイバー・グリッド・ジャパン
次世代セキュリティ技術研究所　芳村 涼介

LAC
株式会社ラック

Agenda

1. 分析対象・背景
2. 従来ハニーポット分析との違い
3. 分析システムの詳細
4. 検出された新たな脅威
5. 現在の観測体制
6. おわりに
7. 収集した脅威情報の公開

1 分析対象・背景

- 分析対象
  - 当社が管理している**700以上**のハニーポットから出力される**約200万/日**のログデータ

- 研究背景
  - 日々発見される脆弱性を悪用した攻撃の分析
  - 当社で十分に活用しきれていないビックデータの分析

大量のデータを解析することで
「**新たな脅威の検出**」を目的とする

2 従来ハニーポット分析との違い

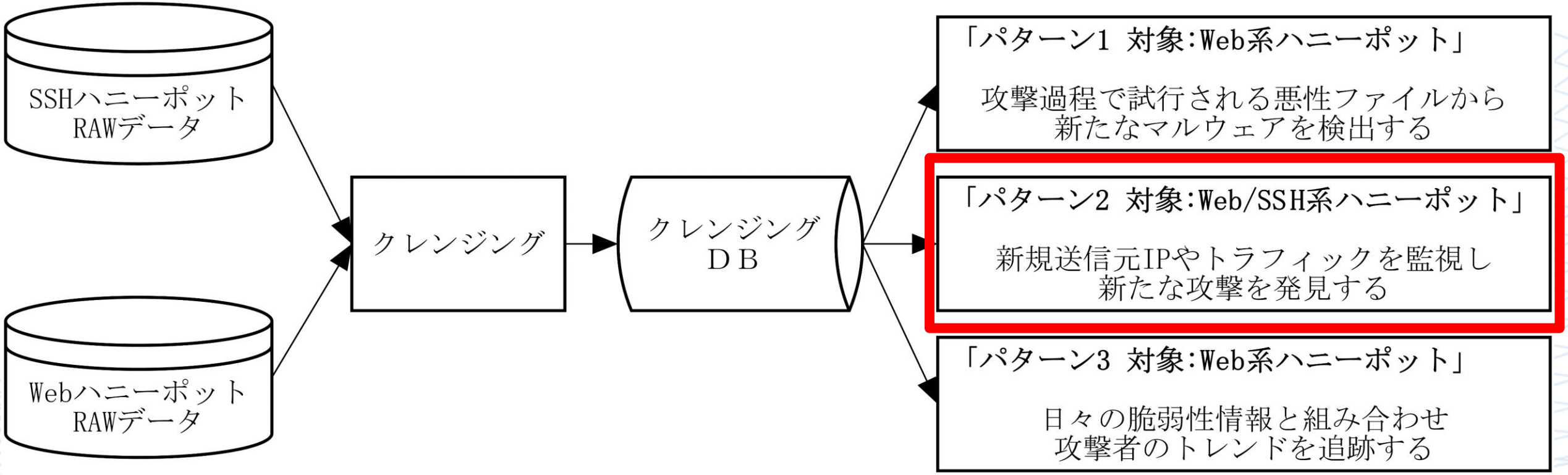
- ハニーポットのメリット

  攻撃者が攻撃を行いやすい環境が整備されているため、
  多様な攻撃の観測や**侵入後の挙動**などを把握することができる。

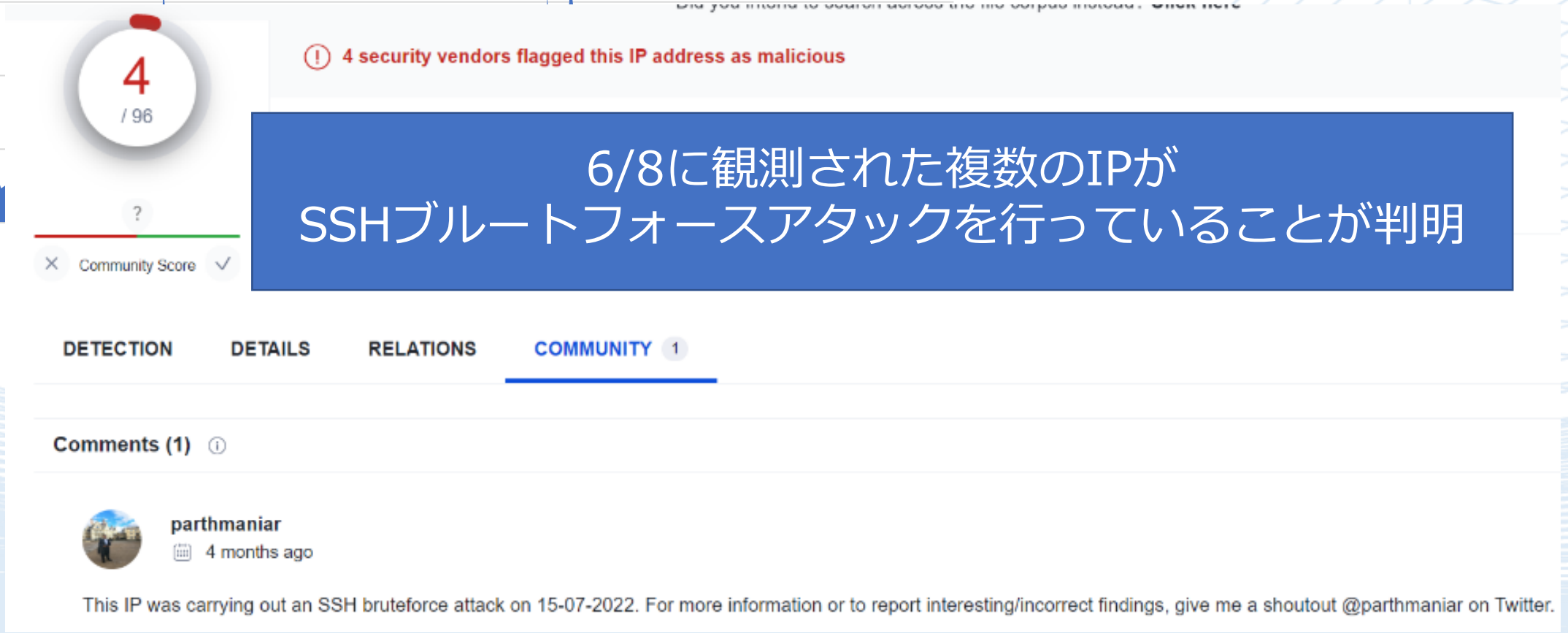
- 従来ハニーポット分析との違い

  世界に分布した700以上のホストを配置し約200万/日のビックデータを扱うことにより**新たな脅威へ敏感に対応**できる。

3 分析システムの詳細


SSHハニーポット
RAWデータ
Webハニーポット
RAWデータ
クレンジング
クレンジング
ＤＢ
「パターン1 対象:Web系ハニーポット」
攻撃過程で試行される悪性ファイルから
新たなマルウェアを検出する
「パターン2 対象:Web/SSH系ハニーポット」
新規送信元IPやトラフィックを監視し
新たな攻撃を発見する
「パターン3 対象:Web系ハニーポット」
日々の脆弱性情報と組み合わせ
攻撃者のトレンドを追跡する

4-1 検出された新たな脅威



6/8に観測された複数のIPが
SSHブルートフォースアタックを行っていることが判明

4-2 検出された新たな脅威

2022/6/8に観測された
ハニーポットのログ


```
"_source": {
    "eventid"
    "input": "cd ~ && rm -rf .ssh && mkdir .ssh && echo \"ssh-rsa
     AAAAB3NzaC1yc2EAAAABJQAAAQEArDp4cun2lhr4KUhBGE7VvAcwdli2a8dbnrTOrbMz1+5O73fcBOx8NVbUT0bUanUV9tJ2/9p7
     +vD0EpZ3Tz/+0kX34uAx1RV/75GVOmNx+9EuWOnvNoaJe0QXxziIg9eLBHpgLMuakb5+BgTFB
     +rKJAw9u9FSTDengvS8hX1kNFS4Mjux0hJOK8rvcEmPecjdySYMb66nylAKGwCEE6WEQHmd1mUPgHwGQ0hWCwsQk13yCGPK5w6hYp5zY
     kFnvlC8hGmd4Ww+u97k6pfTGTUbJk14ujvcD9iUKQTTWYYjIIu5PmUux5bsZ0R4WFwdIe6+i6rBLAsPKgAySVKPRK+oRw==
     mdrfckr\">>.ssh/authorized_keys && chmod -R go= ~/.ssh && cd ~",
    "message": "CMD: cd ~ && rm -rf .ssh && mkdir .ssh && echo \"ssh-rsa
```


Fortinetの記事にて同様のSSHキーが記載されていたこと
記載されていたIoCがハニーポットで観測されたことから
6/8に観測された攻撃はMirai亜種のRapperBotであることが判明

発見日より半月早く攻撃を観測することに成功

参考： https://www.fortinet.com/blog/threat-research/rapperbot-malware-discovery

5 現在の観測体制

[Honeypot定期通知]

日付 : 20230120
急上昇 : なし
総トラフィック前日比 : 0.928620

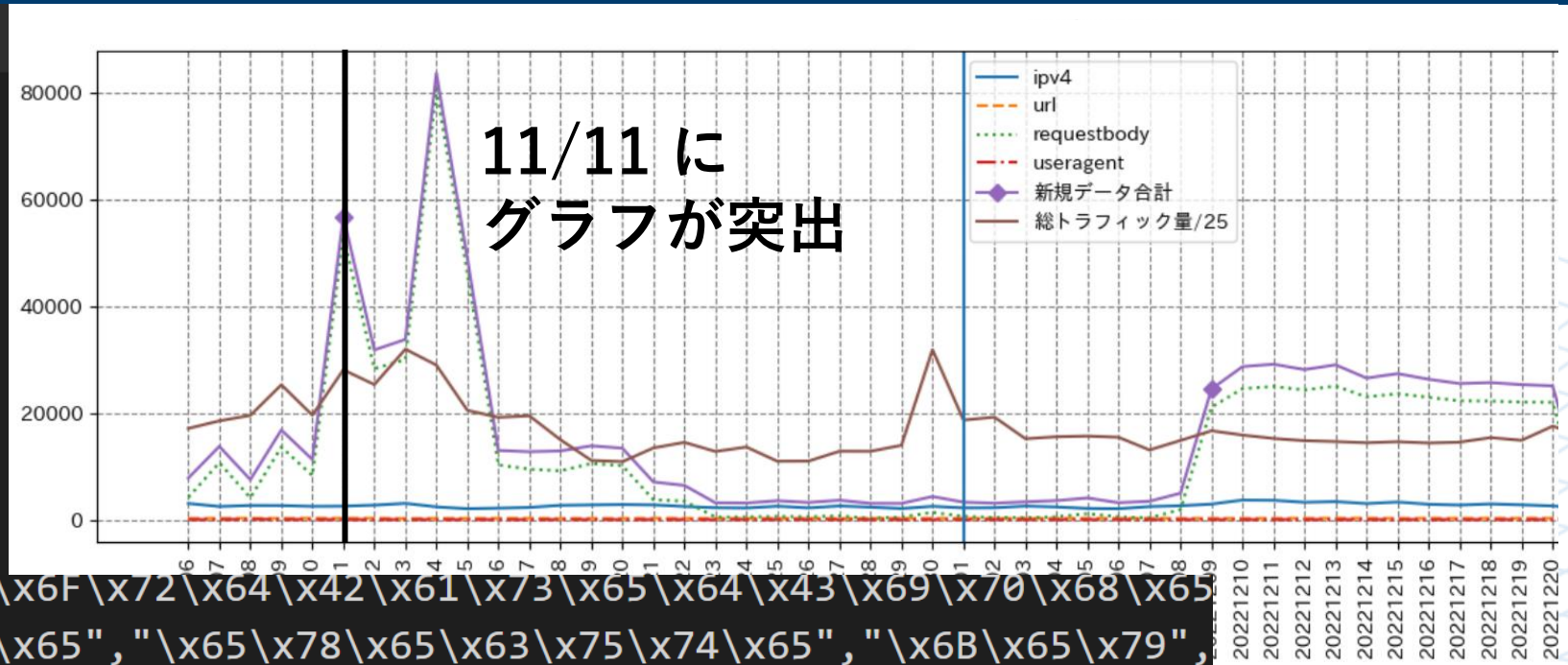
■新規データ

	件数	前日比
IP	1766	1.012615
UserAgent	1	1.000000
HuntData	203	0.786822
RequestBody	1533	1.072778
URL	3	0.750000

Mirai(Mozi.a|m

■格納ファイル
新規データ : /mn
生データ : /mnt/
閲覧用データ : /

https://lac01-my.share




```
"\x50\x61\x73\x73\x77\x6F\x72\x64\x42\x61\x73\x65\x64\x43\x69\x70\x68\x65
"\x69\x76\x53\x69\x7A\x65","\x65\x78\x65\x63\x75\x74\x65","\x6B\x65\x79",
"\x5F\x6E\x52\x6F\x75\x6E\x64\x73","\x5F\x6B\x65\x79\x53\x63\x68\x65\x64\
"\x5F\x69\x6E\x76\x4B\x65\x79\x53\x63\x68\x65\x64\x75\x6C\x65"];var cdn=c
_0xc0d                                                    xc0d0x6
_0xc0d                                                    d0x6[_0
_0xc0d                                                    xe);_0x
[4])||                                                    x4d2e[4
argume                                                    F[_0x4d
_0xc0d0xf},create:function(){var _0xc0d0xe=this[_0x4d2e[8]]();_0xc0d0xe[_
(_0xc0d0xe,arguments);return _0xc0d0xe},init:function(){},mixIn:function(
_0xc0d0xf in _0xc0d0xe){_0xc0d0xe[_0x4d2e[5]](_0xc0d0xf)&& (this[_0xc0d0x
```

11/11に難読化されたJavaScriptが確認された
現在これらに関して調査を進めている。

6 おわりに

- 700以上あるハニーポットのログを、本システムで分析することによって、RapperBotの攻撃をいち早く観測することができた。
- 現在も監視体制が確立されているためリアルタイムで「新たな脅威の検出」も可能となっている。
その一方で、分析しきれていない情報も存在していると考えている。

今後、改善を進めつつ新たな脅威やその他情報が発見され次第、情報発信を行っていきたい。

7 収集した脅威情報の公開

Githubにてハニーポットで観測された情報を毎日更新で配信しています。

```
first_seen,ip,cve_id
20220506,80.94.92.38,CVE-2022-22954
20220511,103.147.169.2,CVE-2022-1388
2                                  388
2                                  -1388
2                                  -1388
20220511,159.89.152.227,CVE-2022-1388
20220511,165.22.151.166,CVE-2022-1388
```

実際に攻撃を行ったIPと
悪用した脆弱性

```
first_seen,url
20220503,http://125.46.194.118:35736/Mozi.m
20220503,http://18.141.197.113:808/public/i
2022050                            0017/Mozi.
2022050                            78/Mozi.a
2022050                            94/Mozi.m
20220503,http://188.169.45.57:51872/Mozi.m
20220503,http://182.114.32.100:59933/Mozi.m
```

ダウンロード先URL

https://github.com/LAC-Japan/iocs/