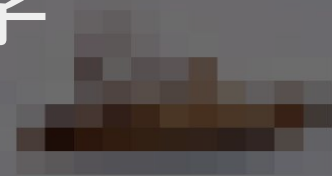


# 100 more behind cockroaches?

or how to hunt IoCs with OSINT

小川 泰明 & 二関 学



# Before Starting

- English version is available for non-native Japanese folks :D



“ゴキブリを1匹見つけたら、  
100匹いると思え”



サイバーの世界にも当てはまる？

A close-up photograph of a baby with light brown hair and a grumpy expression, sitting on a sandy beach. The baby is wearing a green and white long-sleeved shirt and is holding a handful of sand in their right hand. The background is a blurred view of the ocean waves. The word "Yes" is overlaid in white text on the right side of the image.

**Yes**

# ゴキブリキヤッチャー

ゴキブリ捕獲器

コンパクト  
タイプ  
従来サイズの  
2/3  
(当社比)



ならゴキブリホイホイを設置しよう!

簡単タイプ

- 1.よく入るVカット
- 2.強力誘引剤配合(ソトロン)
- 3.タテ置き・ヨコ置き自在
- 4.便利なホイ捨てつまみ

 **KINCHO**

5 セット入

5-06

SOKO HARDWARE

KINCHO

簡単タイプ

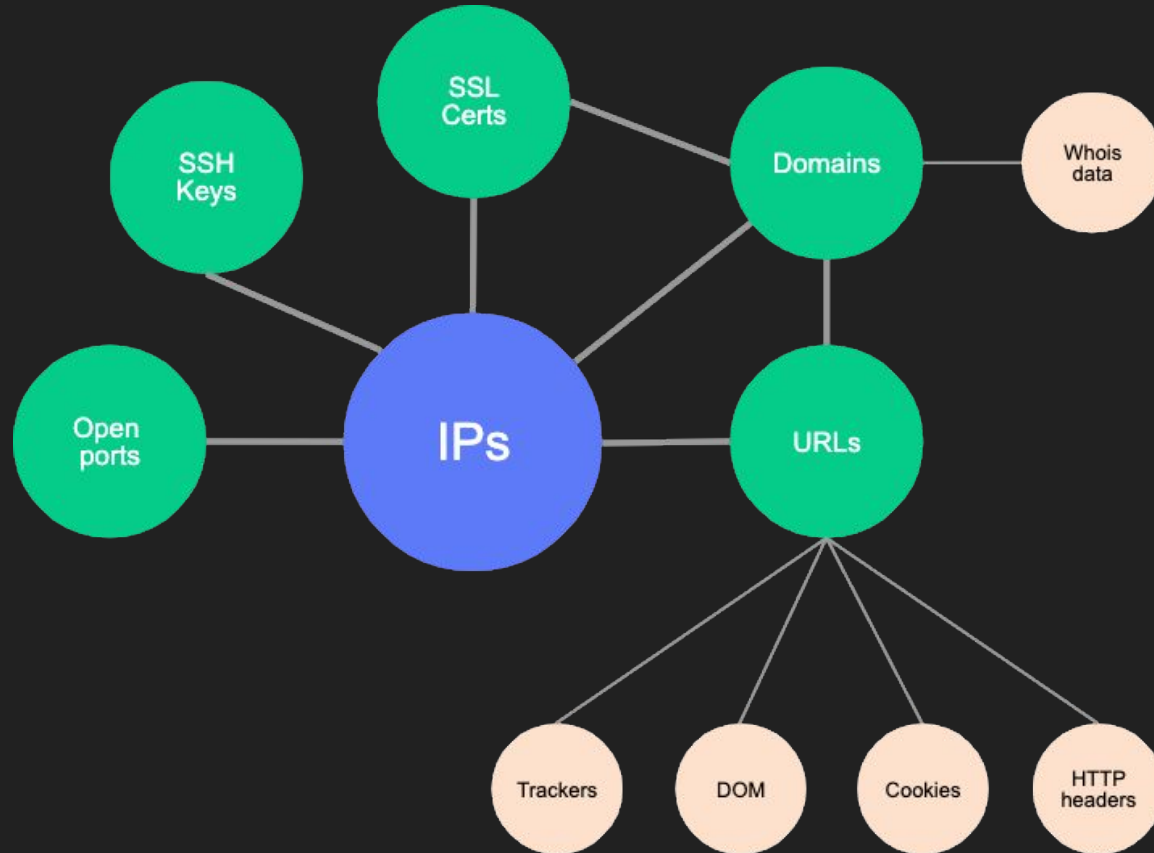
- 1.よく入るVカット
- 2.強力誘引剤配合(ソトロン)
- 3.タテ置き・ヨコ置き自在
- 4.便利なホイ捨てつまみ

# Tracking Fingerprints

- 攻撃者の悪癖:
  - インフラの使い回し
  - コンポーネントの使い回し
  - SSL証明書の使い回し
  - SSHホストキーの使い回し
- 何かを使い回すと、追跡可能性が上がる
  - 犯罪現場に残された指紋のようなもの
  - 指紋をキーにして攻撃者を追跡することが可能



# Fingerprints on the Internet





# Methodologies

- Domain fuzzing
- HTTP fingerprint
- SSH host key fingerprint
- Certificate Transparency
- IoC feeds aggregation
- YARA

# Domain Fuzzing

# Domain Fuzzing

- タイポスクワッシングなドメインを発見するための手法
  - 1 を 2 また q に変換 (手元のQWERTYキーボードを見てみよう)
  - a を à, á, â, ã, ä, å, α, a, ä, ä, à または a に変換
  - 母音(a, e, i, o or u) を別の母音に変換
    - e.g. example.com
      - axample.com, ixample.com, oxample.com, uexample.com, ...
  - などなど
- 見た目が似通ったドメインを見つけることができる



# Domain Fuzzing: MoqHao

# MoqHao

- Androidマルウェア
- DGAライクなドメインを使用する

**ysu3g.xyz**

**hs3dg.xyz**

**nsi3h.xyz**

*/[a-z][a-z][a-z0-9][a-z0-9][a-z]\.xyz/*

# MoqHao

- MoqHaoのホストをドメインファジングで見つける方法
  - スクリプトを自作してみる 😊
    - <https://gist.github.com/ninoseki/8c3b9dd54506691c105c629cd3aa284e>
  - dnstwistを使用する
    - <https://github.com/elceef/dnstwist>

```

$ dnstwist -r hs3dg.xyz

_ _ | _ | _ _ _ _ | _ _ _ _ _ ( _ ) _ _ _ | _ | _
/ _ \ | _ | _ \ _ \ _ \ _ \ _ \ / / / / / | _ | _
| ( | | | | \ _ \ \ _ \ \ \ \ V / / \ _ \ | _ |
\_ \, _ | | | _ _ \ / \ \ / | | _ _ \ / | _ | _ _ \

Processing 846 domain variants ....15%....33%....49%....64%....80%....95%. 3 hits (0%)

Original*      hs3dg.xyz  NS:dns1.registrar-servers.com MX:eforward1.registrar-servers.com
Omission       hsdg.xyz   NS:dns23.hichina.com
Transposition  hsd3g.xyz  162.255.119.169 NS:dns1.registrar-servers.com MX:eforward1.registrar-
servers.com
```

# Certificate Transparency

# Certificate Transparency

- サーバー証明書の発行状況を監視するための仕組みのこと
  - <http://www.certificate-transparency.org/>
  - 雑に言うと、CTを使うと新しく証明書が登録されたドメインを無料で取得できる
- 有用なサービスツール:
  - CertStream
    - <https://certstream.calidog.io/>
    - Near real-time certificate transparency log update stream.
  - Phishing Catcher
    - [https://github.com/x0rz/phishing\\_catcher](https://github.com/x0rz/phishing_catcher)
    - Phishing catcher using CertStream
  - urlscan.io certstream-suspicious feed
    - <https://urlscan.io/search/#task.source%3Acertstream-suspicious>
    - Suspicious domains flying through CertStream





16SHOP

# Certificate Transparency:

16shop

Email

Enter email

Password

Enter password

Remember me

Powered by ZlCoder Team

Login

# 16shop

- AppleとAmazonのユーザーを標的にしたインドネシア製のフィッシングキット
  - Akamai曰く、16shopは“a highly sophisticated phishing kit.”
    - <https://blogs.akamai.com/sitr/2019/05/16shop-commercial-phishing-kit-has-a-hidden-backdoor.html>
  - C2:
    - 128.199.154.155 / 167.99.79.91

# 16shop

- 16shopはHTTPSを使用する?
  - Yes.
    - <https://account-alertautorizher.com>
    - <https://amazon.legal-privacy-comercial.com>
    - <https://appleid.apple.com.accountt-updates.reviews>
    - <https://applesecurityapp.hopto.org>
    - <https://applid.manage-account.information.terdjasilagi.com>
    - <https://apps-amazon.co.jp-logsrvaslo29s.info>
    - <https://bublewrap-tcoapple-api.ddnslive.com>
    - <https://id.amazon.corn.idmsa-authsighin-verify.pakistanapimn.com>
    - <https://mails-amazon.us>
    - etc.

# 16shop

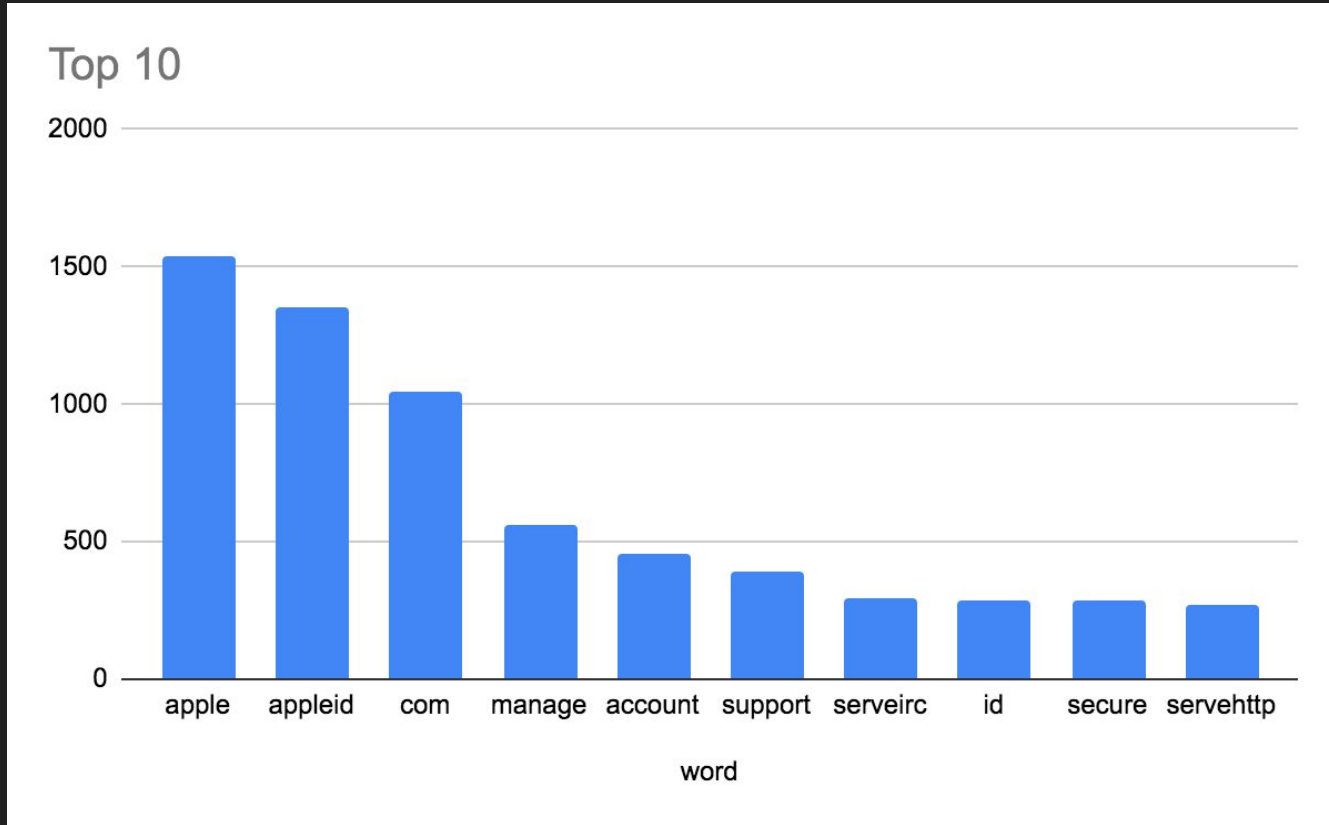
- 6,500+ある16shopのドメインから、単語の出現数を分析してみる

appleid.apple.com.accountt-updates.reviews



appleid apple com accountt updates

# 16shop



# 16shop

- CTログのCNに16shopでよく使われている単語が含まれている場合、16shopである可能性がある
- Webサイトが16shopかどうかは、`/admin/index.php`にアクセスした時のHTTPレスポンスボディのハッシュ値をチェックすることで判断できる
  - 16shop Apple version.
    - `0e06d02dab03e8085b18ebedb0f54dc68508c40c5d1b8c6e3e8da98e3d3b6649`
    - `ce4fe392dd0f996923c5cf272d98e1e2778a2a44ffb2a4435fdb9c13665215f3`
  - 16shop Amazon version.
    - `2edfff035a357aec4cea23057ea2e10af1dd3431713c904cf1cd804640bd2965`

# Omake: Bizarre Domains

- `manage.unauthorized.login.amazon.co.jp.omachikudasai.com`
- `xn--id-zb4axila5esc1e1f9bvhzd4a6fe.manage-konohajp.tokyo(アップルジャパンのログインid.manage-konohajp.tokyo)`
- `appleid.apple.com.xn--ccks5nkb8068afysn7bba.com(appleid.apple.com.本日本国アメリカ.com)`
- `youji-kyoiku.com`

HTTP fingerprint

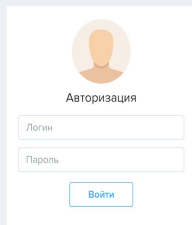


# HTTP Fingerprint: Predator The Thief



# Predator The Thief

- スティーラーマルウェア
- @fumik0\_さんが詳細なレポートを公開している
  - <https://fumik0.com/2018/10/15/predator-the-thief-in-depth-analysis-v2-3-5/>
- Predator The ThiefのC2は静的なHTTPレスポンスを返す



```
<head lang="en">
  <meta charset="UTF-8">
  <meta name="viewport" content="width=device-width, initial-scale=1, user-
scalable=no">
  <meta http-equiv="x-ua-compatible" content="ie=edge">
  <title>Predator The Thief – Нативный стиллер с большим функционалом / Лучшая цена!
- Вход</title>
  <link rel="shortcut icon" href="">
  <!-- HTML5 shim and Respond.js for IE8 support of HTML5 elements and media queries
-->
  <!--[if lt IE 9]>
    <script src="https://oss.maxcdn.com/html5shiv/3.7.2/html5shiv.min.js"></script>
    <script src="https://oss.maxcdn.com/respond/1.4.2/respond.min.js"></script>
  <![endif]-->
  <link href="/upload/css/adminlte.css" rel="stylesheet">
  <link href="https://cdnjs.cloudflare.com/ajax/libs/admin-lte/2.4.8/css/skins/_all-
skins.min.css" rel="stylesheet">
  <link rel="stylesheet" href="/upload/css/login.main.css">
  <link href="https://maxcdn.bootstrapcdn.com/font-awesome/4.4.0/css/font-
awesome.min.css" rel="stylesheet">
  <link
href="https://stackpath.bootstrapcdn.com/bootstrap/4.0.0/css/bootstrap.min.css"
rel="stylesheet">
  <link rel="stylesheet" href="/upload/css/main.min.css">
</head>
...
```

# Predator The Thief

- “静的なHTTPレスポンス”は、常に同じレスポンスを返すことを意味する
  - つまり、HTTPレスポンスのハッシュを指紋として利用できる
- Predator The Thief C2用のクエリ:
  - Censys(SHA256):
    - `b064187ebdc51721708ad98cd89dacc346017cb0fb0457d530032d387f1ff20e`
  - BinaryEdge(SHA256):
    - `b064187ebdc51721708ad98cd89dacc346017cb0fb0457d530032d387f1ff20e`
  - Shodan(MurmurHash3):
    - `http.html_hash:-1467534799`

PANDA

U Name...

P Password...

Remember me

# HTTP Fingerprint: PANDA

# PANDA

- ShadowVoiceによって使用されるC2
  - 韓国FSIがShadowVoiceに関するレポートをBlack Hat Asia 2019で公開している
  - <https://i.blackhat.com/asia-19/Fri-March-29/bh-asia-Jang-When-Voice-Phishing-Met-Malicious-Android-App-updated.pdf>
- PANDAのHTTPレスポンスは静的ではない
  - なぜなら、リソースの読み込みに絶対パスを使用しているから

```
<head>
  <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
  <meta name="viewport" content="width=device-width, initial-scale=1,maximum-scale=1,
user-scalable=no">

  <title>PANDA</title>
  <link rel="icon" type="image/x-icon"
href="http://103.117.137.175/assets/img/favicon.ico">
  <link rel="shortcut icon" type="image/x-icon"
href="http://103.117.137.175/assets/img/favicon.ico">
```

# PANDA

- このため、ハッシュ値による照合は効果がない
- しかし、別のテクニックを使用して見つけることができる
  - フリーテキスト検索、faviconハッシュ、etc.
- PANDA C2用のクエリ:
  - Censys:
    - ("PANDA" AND "SMAdmin" AND "layui")
  - BinaryEdge:
    - ("PANDA" AND "SMAdmin" AND "layui")
  - Shodan:
    - [http.favicon.hash:-633986505](http://http.favicon.hash:-633986505) [http.title:PANDA](http://http.title:PANDA)

# SSH Host Key Fingerprint



● 東京地方検察庁について

交通案内・連絡先 >

捜査に御協力ください >

裁判に御協力ください >

罰金等の納付 >

● 犯罪被害者の方々へ

被害回復給付金支給制度 >

捜査に御協力ください >

お知らせ

東京地方検察庁からのお知らせ一覧 >

電動式移動柵一式（政府調達）に係る公告 >

平成30年度東京地方検察庁ほか2か所における歳入金等の警備輸送業務の入札に係る公告 >

採用情報

立川第二法務総合庁舎で使用する電気に関する政府調達に係る公告 >

平成29年度八丈島区検察庁庁舎修繕工事の入札に係る公告 >

新着情報

東京地方検察庁の更新履歴一覧 >

2017年12月25日

平成30年度東京地方検察庁ほか2か所における歳入金等の警備輸送業務の入札に係る公告 >

2017年12月25日

電動式移動柵一式（政府調達）に係る公告 >

● 関連サイト

法務省 >

Q & A >



裁判員制度



# SSH Host Key Fingerprint: Fake Tokyo Public Prosecutors Office



# Fake Tokyo Public Prosecutors Office

- 東京地方検察庁に偽装した特殊詐欺
- 使用されたWebサーバーは、同じSSHホストキーを使い回していた
- 偽サーバー用のクエリ:
  - Censys(SHA256):
    - `8e60fb30fb9a268b90a3d5af984c9326d3568a2554fc7ae5bfab1eb621c15518`
  - BinaryEdge(MD5):
    - `"f2:03:78:e5:a3:bb:50:6b:32:be:22:ad:52:3e:cc:98"`
  - Shodan(MD5):
    - `f2:03:78:e5:a3:bb:50:6b:32:be:22:ad:52:3e:cc:98`
- Credit to @tiketiketikeke and @catnap707
  - <https://tike.hatenablog.com/entry/2018/07/03/004132>

# IoC Feeds Aggregation

# IoC Feeds

- URLhaus: <https://urlhaus.abuse.ch/>
  - Malware URL exchange by abuse.ch.
  - 情報源:
    - abuse.ch, 個人によるレポート, etc.
- IOC-DB: <https://labs.inquest.net/iocdb>
  - Indicator of Compromise database by InQuest.
  - 情報源:
    - Twitter, GitHub and blogs.
- Twitter IOC Hunter: <http://tweettioc.com/#>
  - Twitter based IoC database/feed by @fatihsirinnnn.
  - 情報源:
    - Twitter

# EMOTET

## IoC Aggregation: Emotet



# Emotet IoC Feeds

- URLhaus:

```
$ curl -X POST https://urlhaus-api.abuse.ch/v1/tag/ -d "tag=emotet"
{
  "query_status": "ok",
  "firstseen": "2018-03-06 15:27:00",
  "lastseen": "2019-12-23 06:00:03",
  "url_count": "92092",
  "urls": [
    {
      "url_id": "275484",
      "url": "http://www.csnsrserver.com/blog/trust.accs.docs.biz/",
      "url_status": "online",
      "dateadded": "2019-12-23 02:33:04",
      "reporter": "zbetcheckin",
      "threat": "malware_download",
      "tags": ["doc", "Emotet", "Heodo"],
```

# Emotet IoC Feeds

- IOC-DB:

```
$ curl "https://labs.inquest.net/api/iocdb/search?keyword=emotet"
{
  "data": [
    {
      "artifact": "rule MAL_Emotet_JS_Dropper_Oct19_1 {\n  meta:\n      description =
\nDetects Emotet JS dropper\"\n      author = \"Florian Roth\"\n      reference =
\nhttps://app.any.run/tasks/aaa75105-dc85-48ca-9732-085b2ceeb6eb/\n      date = \"2019-10-
03\"\n      hash1 = \"38295d728522426672b9497f63b72066e811f5b53a14fb4c4ffc23d4efbbca4a\"\n
      hash2 = \"9bc004a53816a5b46bfb08e819ac1cf32c3bdc556a87a58cbada416c10423573\"\n
strings:\n      $xc1 = { FF FE 76 00 61 00 72 00 20 00 61 00 3D 00 5B 00\n          27
00 }\n      condition:\n          uint32(0) == 0x0076feff and filesize <= 700KB and $xc1 at 0\n}",
      "artifact_type": "yarasignature",
      "created_date": "Fri, 04 Oct 2019 14:08:34 GMT",
      "reference_link": "https://github.com/Neo23x0/signature-base.git",
      "reference_text": "\nrule MAL_Emotet_JS_Dropper_Oct19_1 {\n  meta:\n      description
= \"Detects Emotet JS dropper\"\n      author = \"Florian Roth\"\n      reference..."
    }
  ]
}
```

# Emotet IoC Feeds

- Twitter IOC Hunter:

```
$ curl http://www.tweettioc.com/v1/tweets/daily/ioc/hashtags/emotet
[
  {
    "md5": [],
    "sha1": [],
    "sha256": [],
    "mail": [],
    "ip": [],
    "domain": [
      "hasmob.com"
    ],
    "url": [
      "http://hasmob.com/other/alibaba.com/Login.htm"
    ],
    "tweet": {
      "date": {
        "$date": 1577581873000
      }
    }
  }
]
```

YARA



# YARA

- マルウェアの検知・分類ツール
- YARAを使うことで、同じ文字列やバイナリをもつファイルを大量のサンプルから検知し、分類することが可能



# Where can we use YARA?

- オンラインサービス
  - Hybrid Analysis
    - <https://www.hybrid-analysis.com/>
  - VirusTotal Hunting
    - <https://www.virustotal.com/gui/hunting-overview>
  - Malpedia
    - <https://malpedia.caad.fkie.fraunhofer.de/> (Invitation only)
  - Koodous
    - <https://koodous.com/> (Android malware only)
- YARA command line tool
  - <https://virustotal.github.io/yara/>

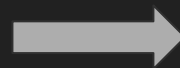
A close-up photograph of a smartphone lying on a laptop keyboard. The phone's screen is illuminated with a dense stream of green text, resembling computer code or a terminal window. The text is slightly blurred, creating a sense of motion or data processing. The keyboard keys are visible in the background, with some like 'T', 'R', 'D', and 'X' being more prominent. The overall lighting is dim, with the green glow from the screen providing the primary light source.

# YARA: MoqHao

# Fake Sagawa Express Mobile Application (MoqHao)

- 佐川急便に偽装したAndroidマルウェア
- MoqHaoを検知するためのYARAルール

```
1 rule MoqHao_regex_MultipleDEX
2 {
3     strings:
4         $a = "AndroidManifest.xml"
5         $b = /classes(\d{1,3}|.*)\.dex/
6         $c = /assets\\S{3,7}\\.S{3,7}/
7     condition:
8         ($a and $c)
9         and #b > 5
10        and filesize < 500KB
11 }
```

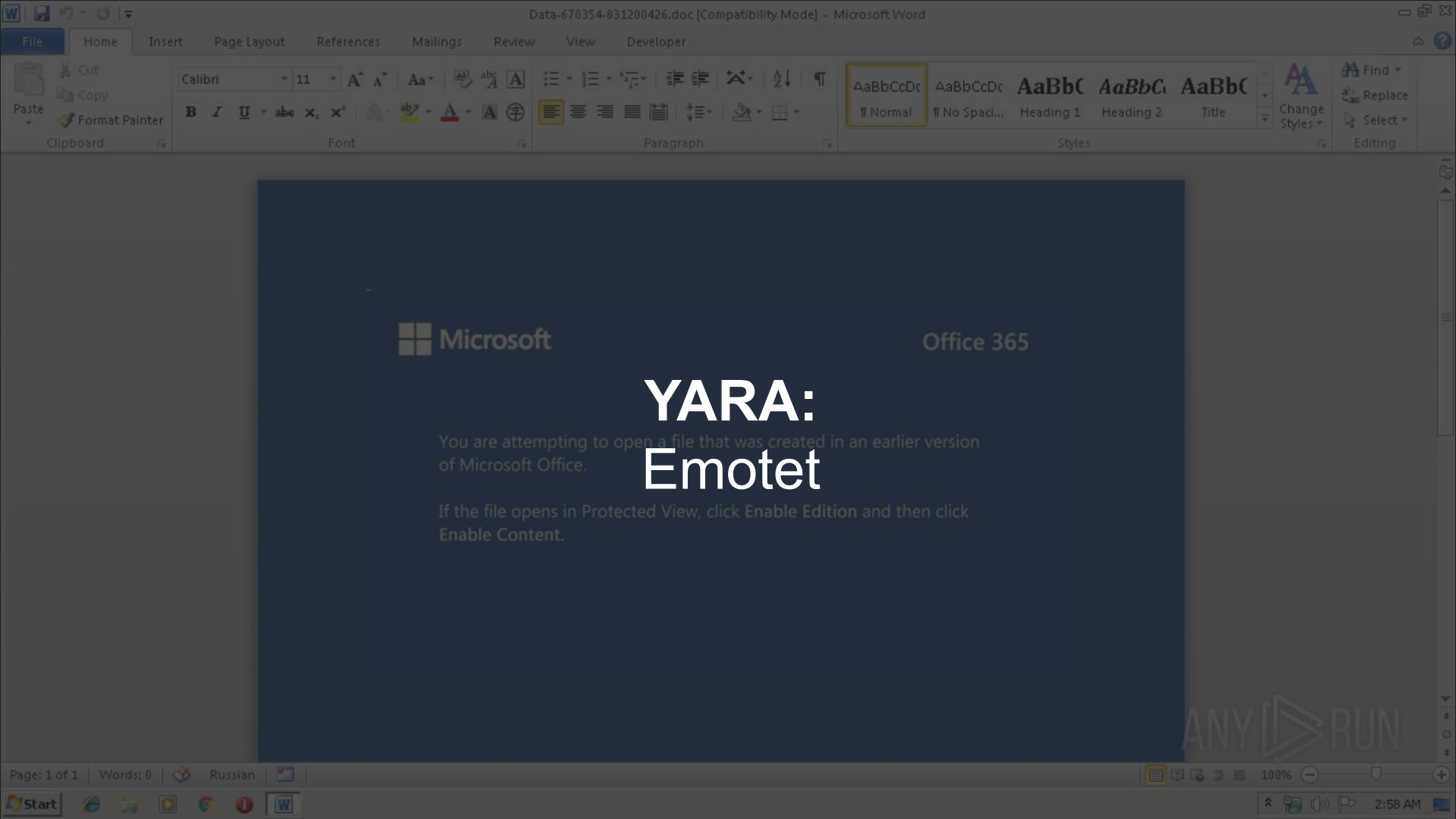


VT hunting  
に登録

# Results of VT Hunting with a YARA rule for MoqHao

b1b61af17218183f12a1d95880ad705dabb8035ac763974f57264714856e84d9 EKOHT3.6.6.apk	MoqHao_regex_MultipleDE X MoqHao	21 / 61	444.60 KB	2019-12-23 15:34:26	2019-12-23 17:25:21	1	
b8883ab4f78dbe407bee6ba8358bbd9030b2242f927caca5c6928f1b7beaea58 smartcat.apk	MoqHao_regex_MultipleDE X MoqHao	21 / 61	444.60 KB	2019-12-09 16:29:02	2019-12-23 15:48:42	1	
c803b2da50761d0df47246434103fe4eab2c9fb76da13871a9b0006ad2b3bb39 smartcat.apk	MoqHao_regex_MultipleDE X MoqHao	22 / 62	435.18 KB	2019-12-09 08:21:34	2019-12-23 15:44:59	1	
3371118f72444fa2adacaf019c97e0f46d9fbc600117ed0bae99f3e3119fc4a8 /sagawa4.2.5.apk	MoqHao_regex_MultipleDE X MoqHao	13 / 63	453.47 KB	2019-12-23 04:11:31	2019-12-23 05:13:47	1	
b92964a7025b3dff864d6604c0b3efa9da4d73b5d3b6bed291558c6506237361 /sagawa9.4.7.apk	MoqHao_regex_MultipleDE X MoqHao	13 / 63	447.05 KB	2019-12-23 03:14:07	2019-12-23 04:16:55	1	
6c5550872466bde72d217c6bda8cf77372f0de256a8bdc4ceda7c0c5bf906498 /sagawa8.8.9.apk	MoqHao_regex_MultipleDE X MoqHao	13 / 63	447.05 KB	2019-12-23 03:12:30	2019-12-23 04:14:36	1	
2267227bc63e3b3660cada35e854f33075de3644adf62ecfae0b966d02a2ca03 yHxnzDyRoEyyN7uMPva420191223-36210-15tg5al	MoqHao_regex_MultipleDE X MoqHao	15 / 64	450.05 KB	2019-12-23 02:21:56	2019-12-23 03:23:10	1	
4b365e1ff416250156d65233e0a53ce99b1f4b75f448cc2ffe24cc93832893cd /sagawa9.3.8.apk	MoqHao_regex_MultipleDE X MoqHao	15 / 64	450.28 KB	2019-12-23 02:08:23	2019-12-23 03:10:44	1	
21b238c28eace817e253071281c0859e0eb263b3285e4115af66b5c0b31a8007 /sagawa9.3.8.apk	MoqHao_regex_MultipleDE X MoqHao	15 / 64	450.28 KB	2019-12-23 01:16:04	2019-12-23 02:17:00	1	
6382c9a99c6e4b8c1314bce6a135cc8e38d878992f1c5fa94cb7fda7e2e3b342 /sagawa9.3.8.apk	MoqHao_regex_MultipleDE X MoqHao	15 / 64	450.28 KB	2019-12-23 01:10:34	2019-12-23 02:11:36	1	

佐川急便以外の亜種のMoqHaoも自動的に捕捉することができる



Cut Copy Paste Format Painter  
Clipboard

Calibri 11 A A Aa abc A  
B I U abc x x² A ab A  
Paragraph

AaBbCcDc AaBbCcDc AaBbC AaBbC AaBbC  
Normal No Spaci... Heading 1 Heading 2 Title  
Change Styles Find Replace Select Editing



Office 365

# YARA: Emotet

You are attempting to open a file that was created in an earlier version of Microsoft Office.

If the file opens in Protected View, click Enable Edition and then click Enable Content.



# Emotet

- 特徴的な文字列がEmotetの中にある

```
00 00-62 61 64 20 61 6C 6C 6F nFrame..bad allo
00 00-FC 2A 43 00 D4 00 00 00 cation...*C.....
40 00-B0 44 43 00 00 00 00 00 ....`-@..DC....
43 00-D0 29 40 00 ED CA 41 00 .....}C..)@...A.
73 20-44 65 66 65 6E 64 65 72 Windows Defender
64 20-53 65 63 75 72 69 74 79 Stupid Security
7A 74-68 23 7D 32 7E 61 52 59 :)..q*zth#}2~aRY
25 61-53 4A 71 45 61 3F 54 3F rE72qD%aSjQeA?T?
4E 6B-5A 67 3D 00 57 49 4E 44 E...eGNkZg=.WIND
40 00-9C 2B 43 00 00 00 00 00 IR....@..+C.....
00 00-00 00 00 00 00 00 00 00 .....
00 00-80 7D 43 00 20 2C 40 00 .....}C.,@.
```

MD5:f8105a0e4af7d61006e5e3974710daf3

```
bad allocation
Windows Defender Stupid Security:)
aRYrE72qD%aSjQeA
```

この文字列をベースにYARAルールを作成

```
1 rule emotet
2 {
3     meta:
4         date = "2019-12-17"
5         Family = "Emotet"
6     strings:
7         $a = "Windows Defender Stupid Security"
8     condition:
9         (uint16(0) == 0x5A4D)
10        and $a
11 }
```

このYARAルールでEmotetを捕捉してみよう

# Search result of Hybrid Analysis with YARA rule for Emotet

Timestamp	File Name / URL	Matched Extracted File	Malicious
December 17th 2019 06:56:57 (UTC)	ご入金額の通知・ご請求書発行のお願い 1065821 2019_12_17.doc Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.1, Co ...	Matched Extracted File <28fe30e9...f173de8d> Matched Extracted File <8d8de003...349e6186>	malicious
December 17th 2019 06:40:50 (UTC)	ba3a0eb3-20a0-44bd-9e85-9286ab4c3069 Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.1, Co ...	Matched Extracted File <6196278f...f9b58b09>	malicious
December 17th 2019 06:36:30 (UTC)	http://aimeept.com/wp-includes/INC/lp-2884648-38128-qqew-hxrig8/ Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.1, Co ...	Matched Extracted File <684c1624...1c3e684a>	malicious
December 17th 2019 06:20:49 (UTC)	07458bbf-3550-4369-808a-eac37e05c2f4 Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.1, Co ...	Matched Extracted File <684c1624...1c3e684a>	malicious
December 17th 2019 06:12:58 (UTC)	http://df.jaskot.pl/wp-includes/common_qWq4ce2EE_pcYqFIO3/security_profile/uzfdm44nlf8wx_85v4073s2/ Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.1, Co ...	Matched Extracted File <30b88a06...3d65d43c>	malicious
December 17th 2019 06:11:04 (UTC)	http://voyeur-jp.com/wp-content/7hd-f8v1-49/ Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.1, Co ...	Matched Extracted File <8d8de003...349e6186>	malicious
December 17th 2019 06:10:09 (UTC)	https://saca.vn/wp-admin/private-57180712944-meltXjQ/86563129646-uwpiUsxj-warehouse/nihw-20uyw323y3yss/ Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.1, Co ...	Matched Extracted File <30b88a06...3d65d43c>	malicious

## Considerations:

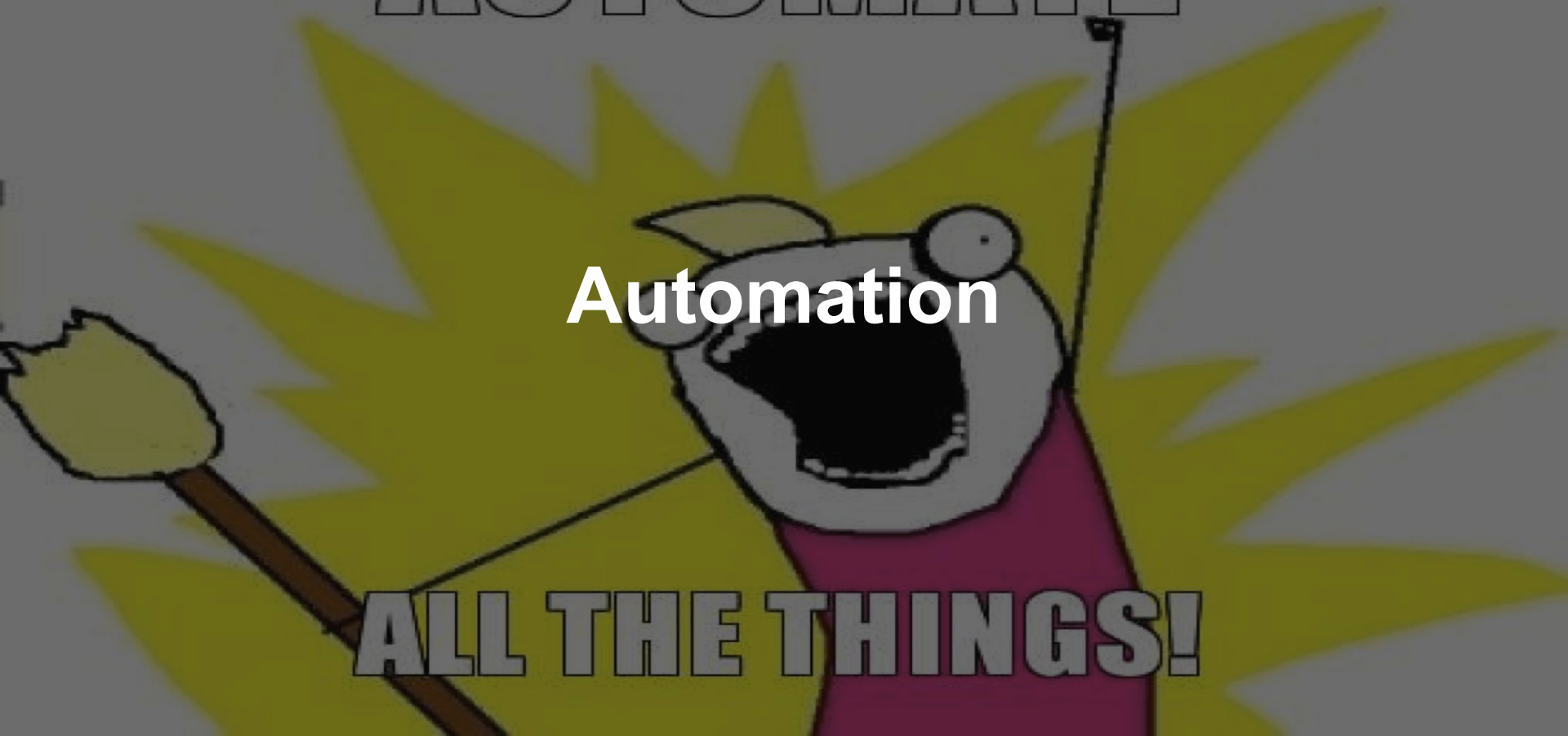
- Hybrid Analysisには38個のサンプルがあり、2019/12/16から2019/12/17にかけて使用されていた



**AUTOMATE**

**Automation**

**ALL THE THINGS!**



# Automation

- なぜ自動化が重要なのか
  - 自動化により運用コストが削減できる
  - 自動化により人的エラーが削減できる
  - 何かを自動化させるのは面白い 😊



# Automation

- Apullo:
  - ネットワーク関連のフィンガープリントを取得するためのツール
  - <https://github.com/ninoseki/apullo>
- Mihari:
  - Shodan, Censys, BinaryEdge等を活用したモニタリングツール
  - <https://github.com/ninoseki/mihari>
- InQuest/ThreatIngestor:
  - IoCを抽出し、集約するためのツール
  - <https://github.com/InQuest/ThreatIngestor>

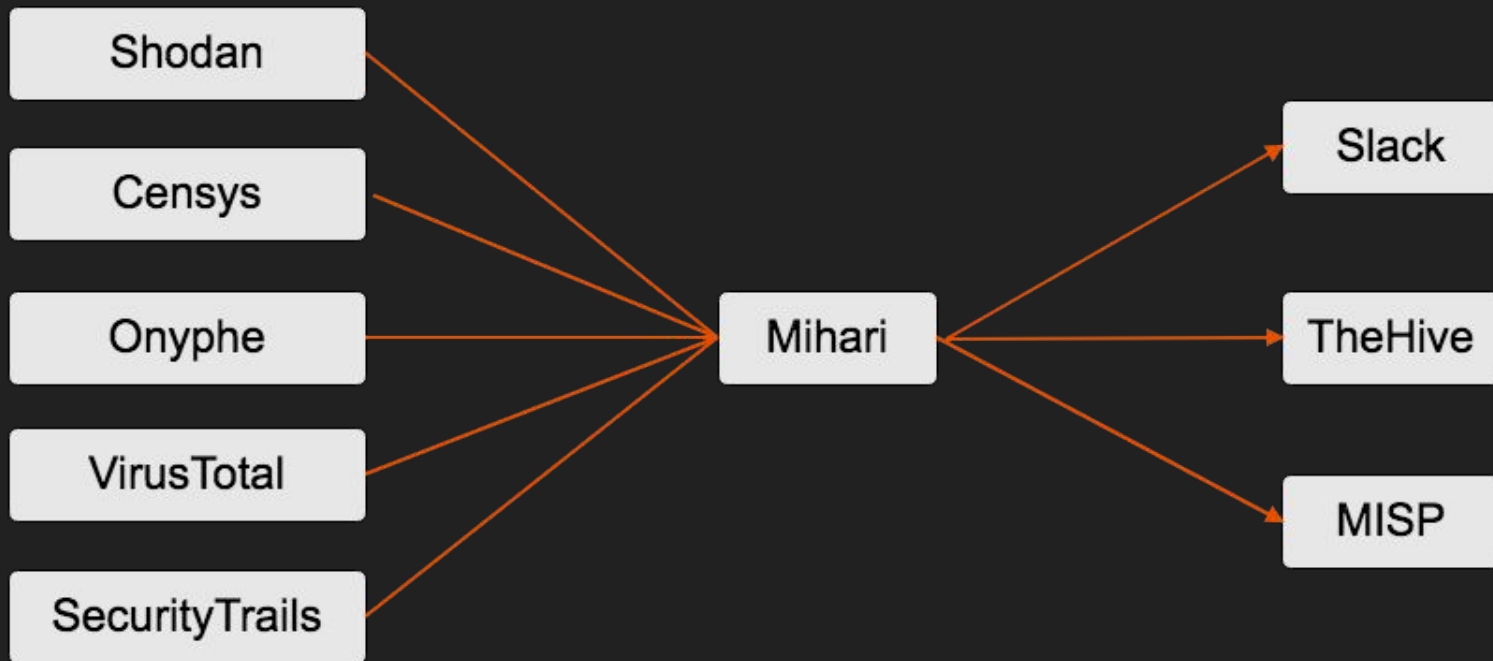
# Apullo

- ネットワーク関連のフィンガープリントを取得するためのツール
  - HTTPレスポンスのハッシュ
  - faviconのハッシュ
  - SSHホストキーのハッシュ
  - WHOIS
  - DNSレコード

```
$ apullo check jppost-be.top
{
  "http": {
    "body": {
      "md5": "74ad15c4ab3f67eee1d546e22248931f",
      "mmh3": -330759974,
      "sha1": "c0280893956852b0c07ae4da752ee5d776d248b8",
      "sha256": "28fa3b0beaf188d48b32557fa4df8f0aa451bd10f8e8bb26e919009d2d41b8fb"
    },
    "cert": {
    },
    "favicon": {
      "md5": "ad184c25a1a01d97696dcb59a1ffef74",
      "mmh3": 111036816,
      "sha1": "cb4842a54c3e96408765290cb810793302c17f0b",
      "sha256": "6949c58f841fa21a89e2e2375ae5645e1db62385f89a0218766f2b0a9c490fb8",
      "meta": {
        "url": "https://www.post.japanpost.jp/img/common/touch-icon.png"
      }
    }
  },
  ...
}
```

# Mihari

- 検索エンジンに問い合わせを行い、その結果に応じてアラートを通知するためのモニタリング用ヘルパー

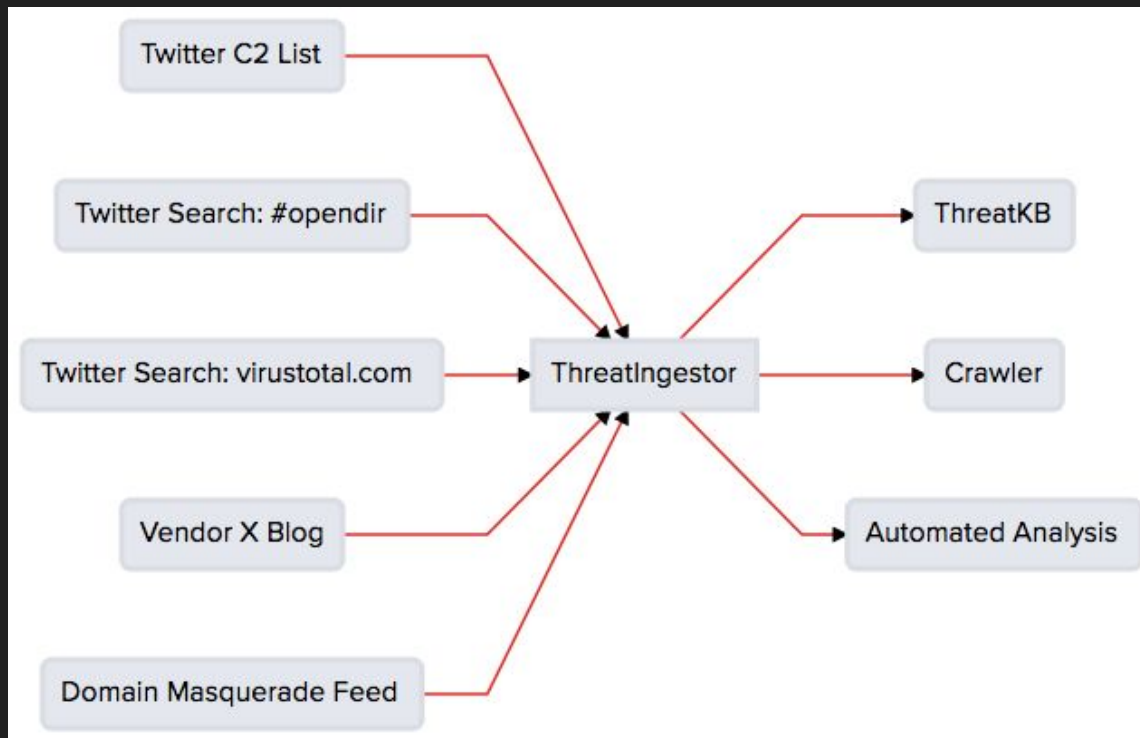


# Mihari

- 対応しているテクニック:
  - Domain fuzzing:
    - dnstwister
  - Passive DNS:
    - SecurityTrails, PassiveTotal, VirusTotal, Pulsedive, CIRCL passive DNS
  - HTTP fingerprint:
    - Shodan, Censys, BinaryEdge, Onyphe, ZoomEye
  - SSH host key fingerprint:
    - Shodan, Censys, BinaryEdge
  - Certificate Transparency:
    - Crt.sh
- Demo

# ThreatIngestor

- InQuestのIOC-DBを支えるデーモン

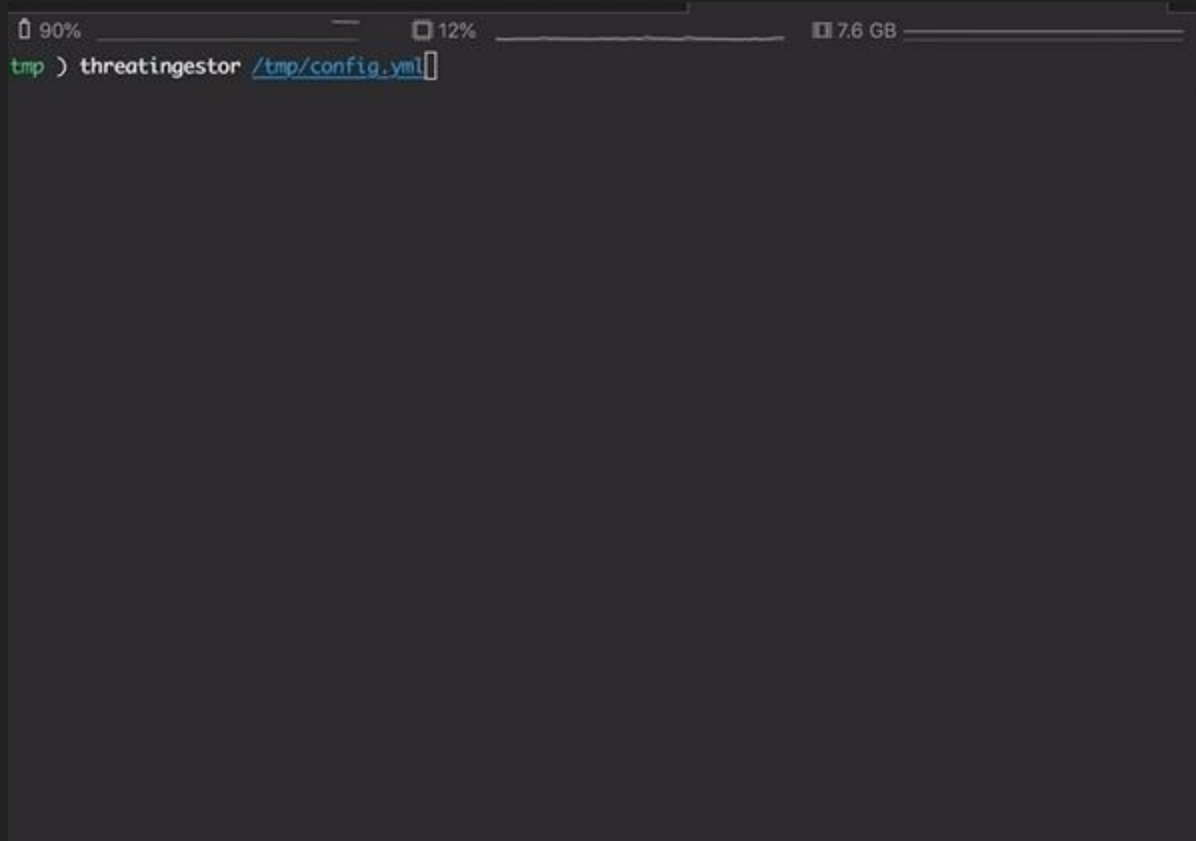


# ThreatIngestor

- 対応しているソース:
  - Twitter, Git repositories, RSS feeds, Generic web pages, etc.
- 対応している出力形式:
  - CSV files, MISP, MySQL, SQLite, ThreatKB, etc.
- iocextractによる強力なスクレイピング機能
  - <https://github.com/InQuest/python-iocextract>
- 超シンプルなWeb UIがビルトインされている
- Demo



# ThreatIngestor



A terminal window with a dark background. At the top, there are three status indicators: a battery icon at 90%, a CPU icon at 12%, and a memory icon at 7.6 GB. Below these, the terminal prompt is 'tmp ) threatingestor /tmp/config.yml' with a cursor at the end of the line.

```
tmp ) threatingestor /tmp/config.yml
```

Conclusion

# Conclusion

- 攻撃者は悪癖により足跡を残す
  - OSINTを支える技術を知る事で、攻撃者の追跡が可能
- 自動化は重要
  - 調査の抜け漏れの低減
  - 属人的になりやすい調査手法の統一化
  - 調査に係る工数(コスト)の削減
- 技術を知り自動化を実現することで、独自のインテリジェンスを生み出せる

# References

- Shodan的http.favicon.hash语法详解与使用技巧
  - <https://www.cnblogs.com/miaodaren/p/9177379.html>
- The Evolution of XLoader and FakeSpy Two Interconnected Android Malware Families
  - <https://documents.trendmicro.com/assets/pdf/wp-evolution-of-xloader-and-fakespy-two-interconnected-android-malware-families.pdf>
- Predator The Thief: In-depth analysis (v2.3.5)
  - <https://fumik0.com/2018/10/15/predator-the-thief-in-depth-analysis-v2-3-5/>
- When Voice Phishing met Malicious Android App
  - <https://i.blackhat.com/asia-19/Fri-March-29/bh-asia-Jang-When-Voice-Phishing-Met-Malicious-Android-App-updated.pdf>
- 16SHOP: COMMERCIAL PHISHING KIT HAS A HIDDEN BACKDOOR
  - <https://blogs.akamai.com/sitr/2019/05/16shop-commercial-phishing-kit-has-a-hidden-backdoor.html>
- 東京地方検察庁の偽サイトを使用した特殊詐欺について
  - <https://tike.hatenablog.com/entry/2018/07/03/004132>

# Image Sources

- P1: <https://www.pexels.com/photo/background-cockroach-shoes-601257/>
- P3: <https://pxhere.com/en/photo/1059154>
- P4: <https://www.flickr.com/photos/christiaancolen/20607150556>
- P5: [https://en.wikipedia.org/wiki/Success\\_Kid](https://en.wikipedia.org/wiki/Success_Kid)
- P6: <https://www.flickr.com/photos/genista/246042481/>
- P12:  
<https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/12/07085742/abstract-mobile.jpeg>
- P36: <https://www.bankinfosecurity.com/emotet-botnet-shows-signs-revival-a-12964>

# List: Tools/Services

Domain Fuzzing		
dnstwist	<a href="https://github.com/elceef/dnstwist">https://github.com/elceef/dnstwist</a>	OSS
Certificate Transparency		
CertStream	<a href="https://certstream.calidog.io/">https://certstream.calidog.io/</a>	OSS
Phishing Catcher	<a href="https://github.com/x0rz/phishing_catcher">https://github.com/x0rz/phishing_catcher</a>	OSS
urlscan.io certstream-suspicious feed	<a href="https://urlscan.io/search/#task.source%3Acertstream-suspicious">https://urlscan.io/search/#task.source%3Acertstream-suspicious</a>	Free service
HTTP Fingerprint / SSH Host Key Fingerprint		
Censys	<a href="https://censys.io/">https://censys.io/</a>	Paid service(has free quota)
BinaryEdge	<a href="https://www.binaryedge.io/">https://www.binaryedge.io/</a>	Paid service(has free quota)
Shodan	<a href="https://shodan.io">https://shodan.io</a>	Paid service(has free quota)

# List: Tools/Services

IoC Feeds Aggregation		
urlhaus.abuse.ch	<a href="https://urlhaus.abuse.ch/">https://urlhaus.abuse.ch/</a>	Free service
IOC-DB	<a href="https://labs.inquest.net/iocdb">https://labs.inquest.net/iocdb</a>	Free service
Twitter IOC Hunter	<a href="http://tweettioc.com/#">http://tweettioc.com/#</a>	Free service
YARA		
Hybrid Analysis	<a href="https://www.hybrid-analysis.com/">https://www.hybrid-analysis.com/</a>	Paid service(has free quota)
VirusTotal Hunting	<a href="https://www.virustotal.com">https://www.virustotal.com</a>	Paid service
Automation		
Apullo	<a href="https://github.com/ninoseki/apullo">https://github.com/ninoseki/apullo</a>	OSS
Mihari	<a href="https://github.com/ninoseki/mihari">https://github.com/ninoseki/mihari</a>	OSS
InQuest/ThreatIngestor	<a href="https://github.com/InQuest/ThreatIngestor">https://github.com/InQuest/ThreatIngestor</a>	OSS