100 more behind cockroaches?

or how to hunt IoCs with OSINT

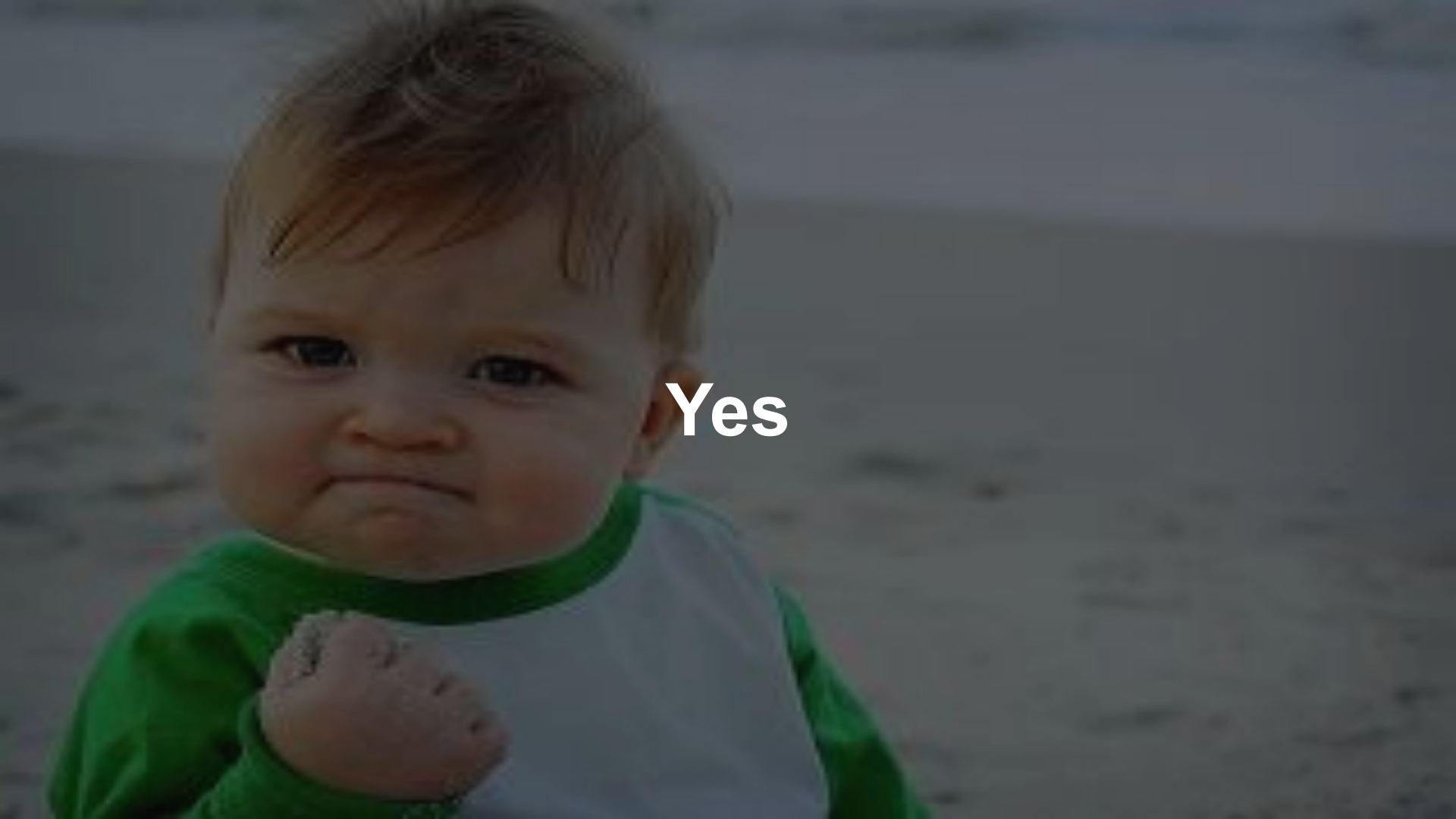
小川 泰明 & 二関 学

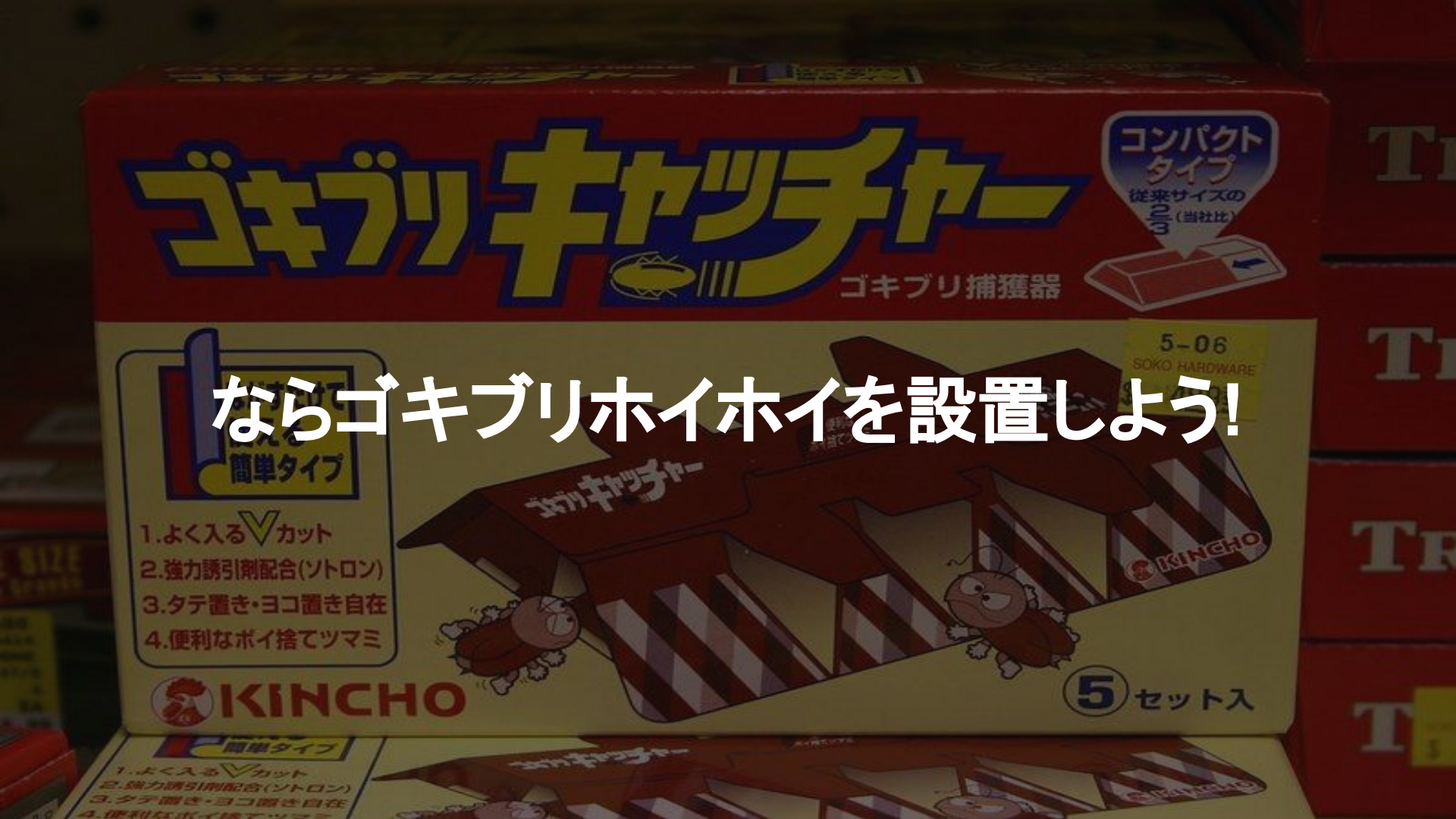
Before Starting

- 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?


Yes

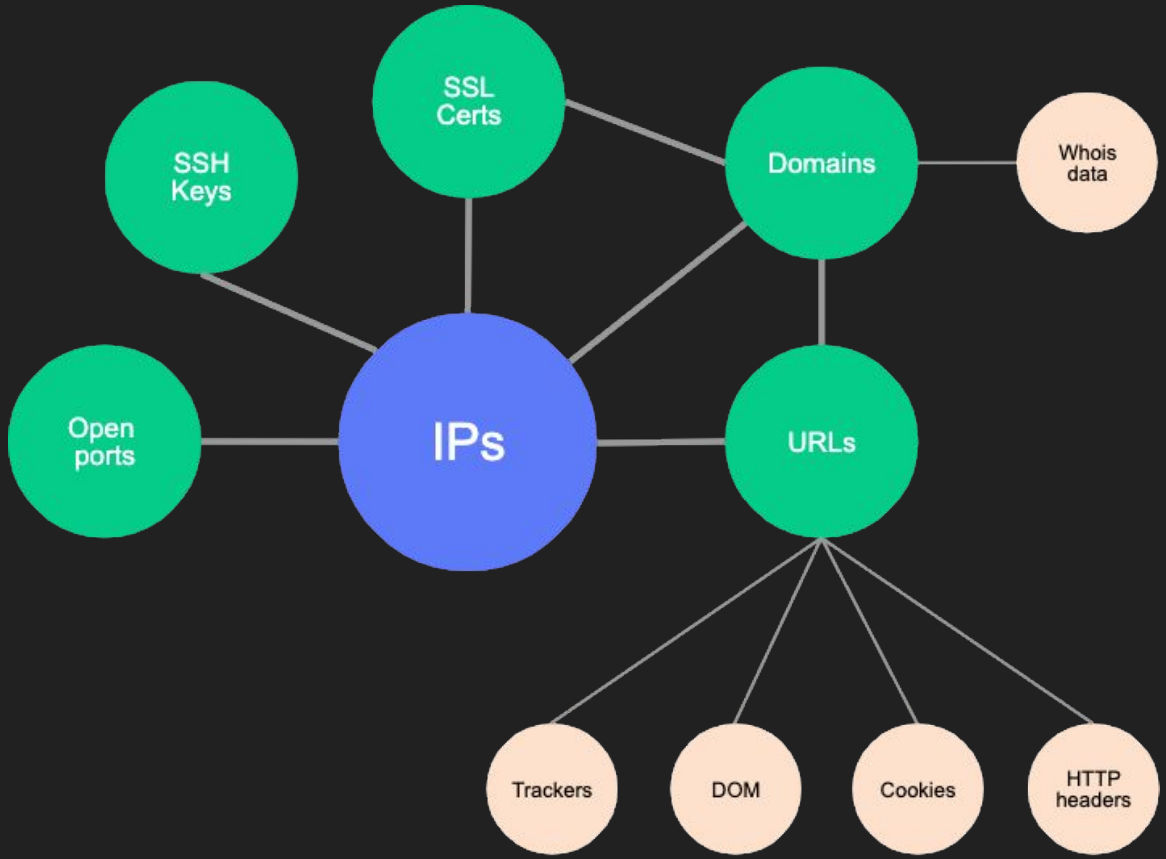


ならゴキブリホイホイを設置しよう!

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

- タイポスクワッティ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**, **ɑ**, **ạ**, **ǎ**, **ă**, **ȧ** または **ą** に変換
  - 母音(**a, e, i, o** or **u**) を別の母音に変換
    - e.g. example.com
      - **a**xample.com, **i**xample.com, **o**xample.com, **u**xample.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

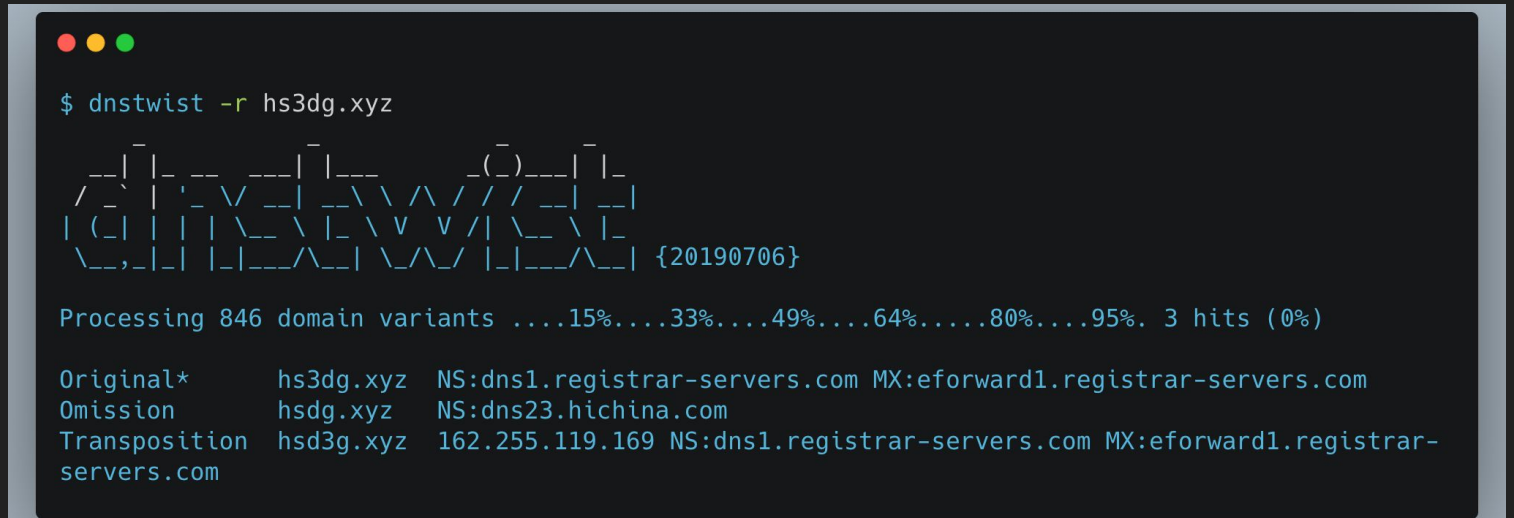
hs3dg.xyz

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



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
    - Phishing catcher using CertStream
  - urlscan.io certstream-suspicious feed
    - https://urlscan.io/search/#task.source%3Acertstream-suspicious
    - Suspicious domains flying throught CertStream

Certificate Transparency: 16shop

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.

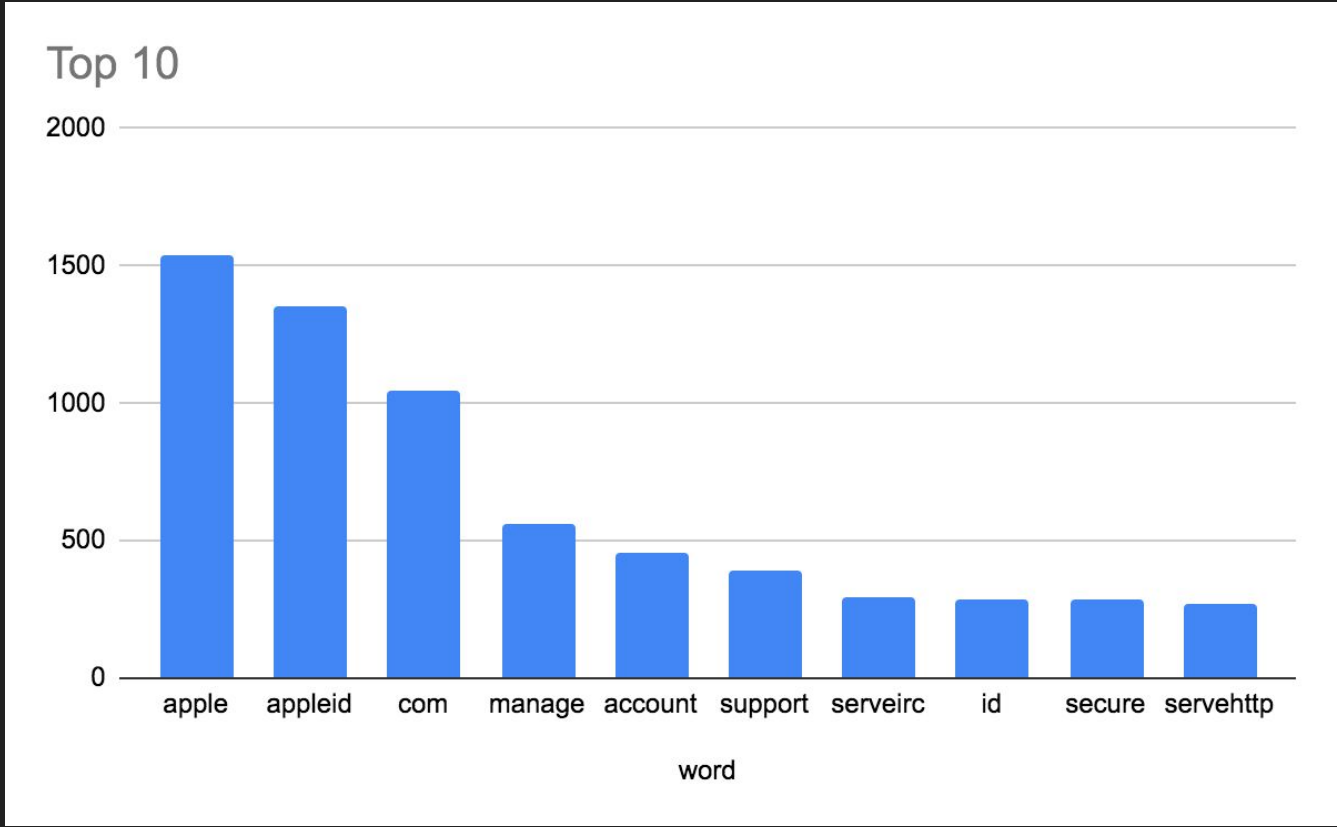
16shop

- 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


Top 10
2000
1500
1000
500
0
apple
appleid
com
manage
account
support
serveirc
id
secure
servehttp
word

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

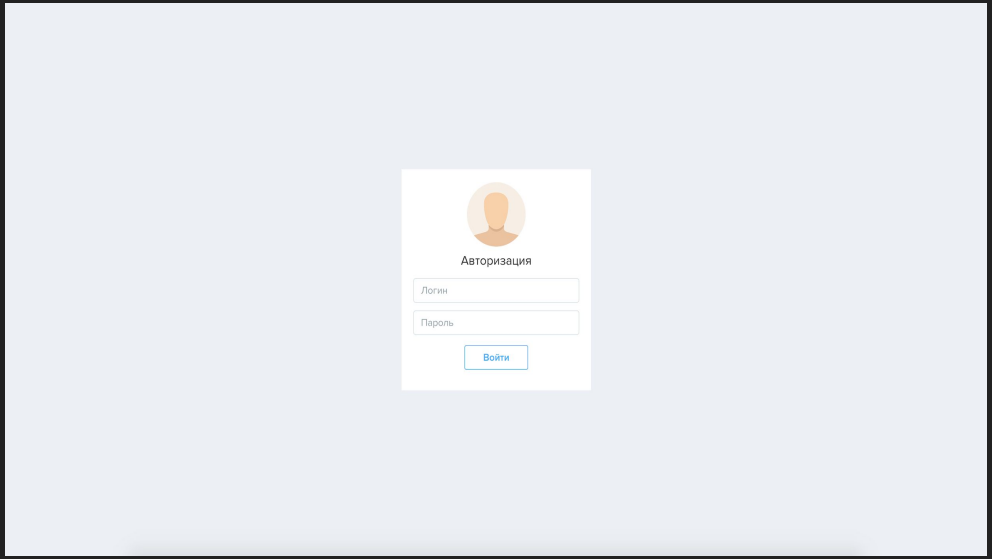
- manage.unauthorized.login.amazon.co.jp.omachikudasai.com
- xn--id-zb4axila5esc1e1f9bvhzd4a6fe.manage-konohajp.tokyo(アップルジャパンのログインid.manage-konohajp.tokyo)
- appleid.apple.com.xn--ccks5nkb8068afysn7bba.com(appleid.apple.com.本日本国アメリカ.com)
- youji-kyoiku.com

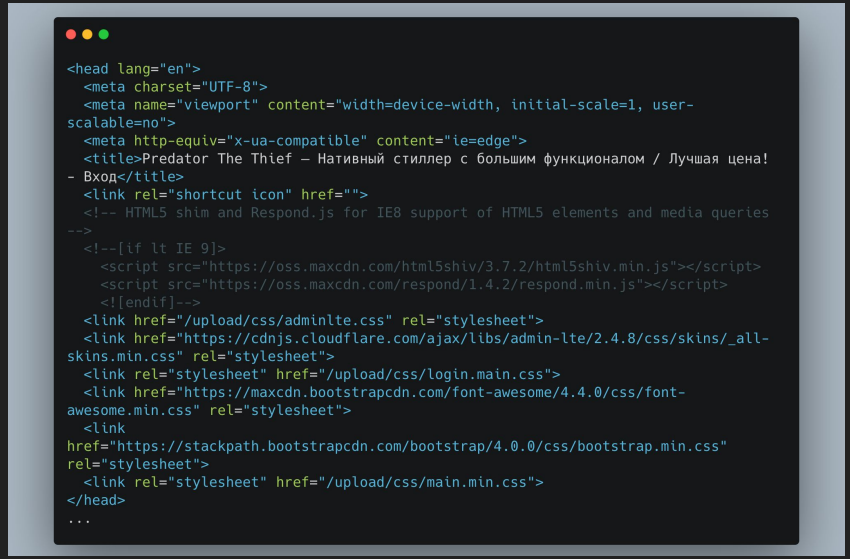
HTTP fingerprint

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

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.title:PANDA

SSH Host Key Fingerprint

SSH Host Key Fingerprint:

Fake Tokyo Public Prosecutors Office

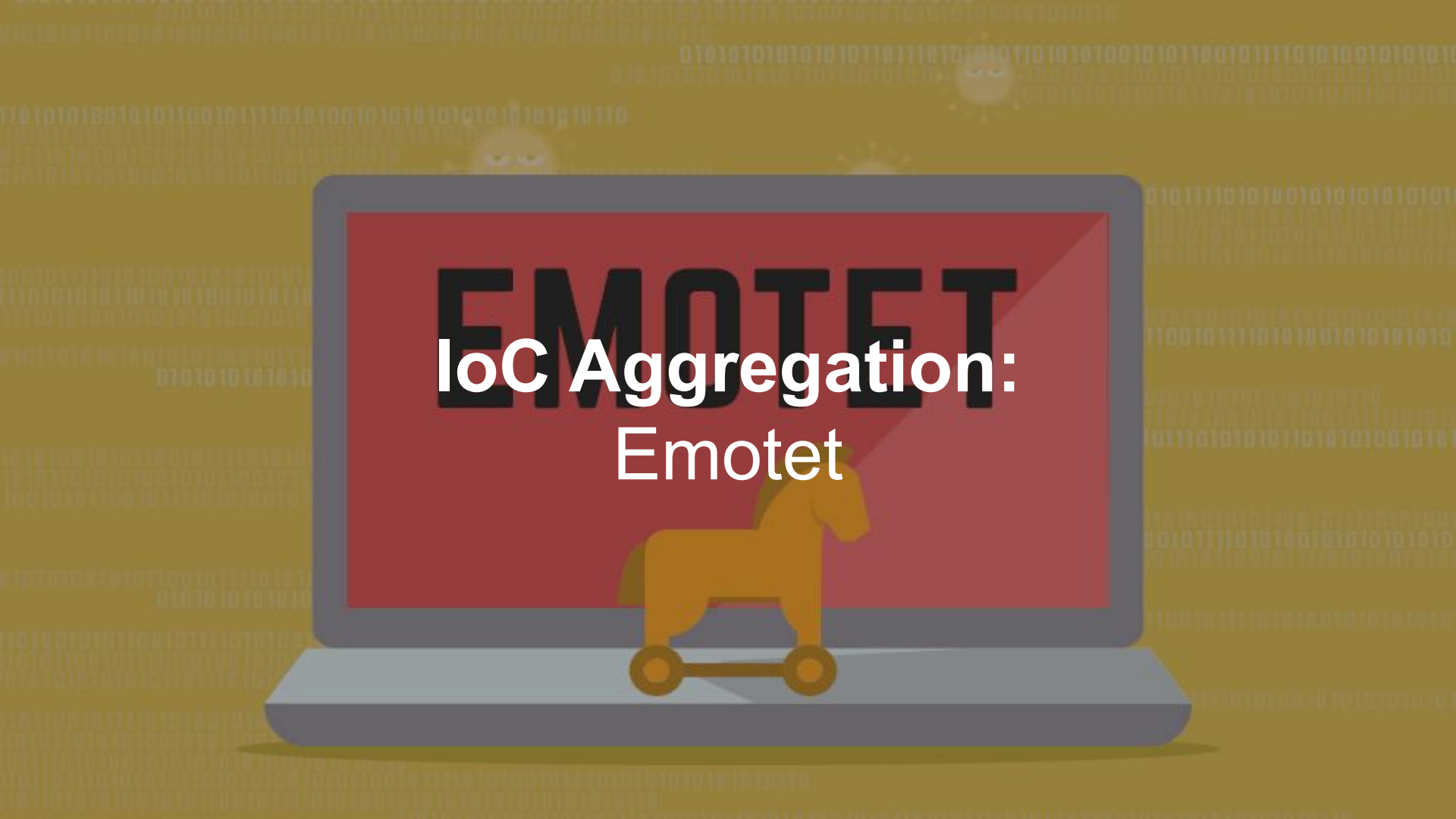
Fake Tokyo Public Prosecutors Office

- 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

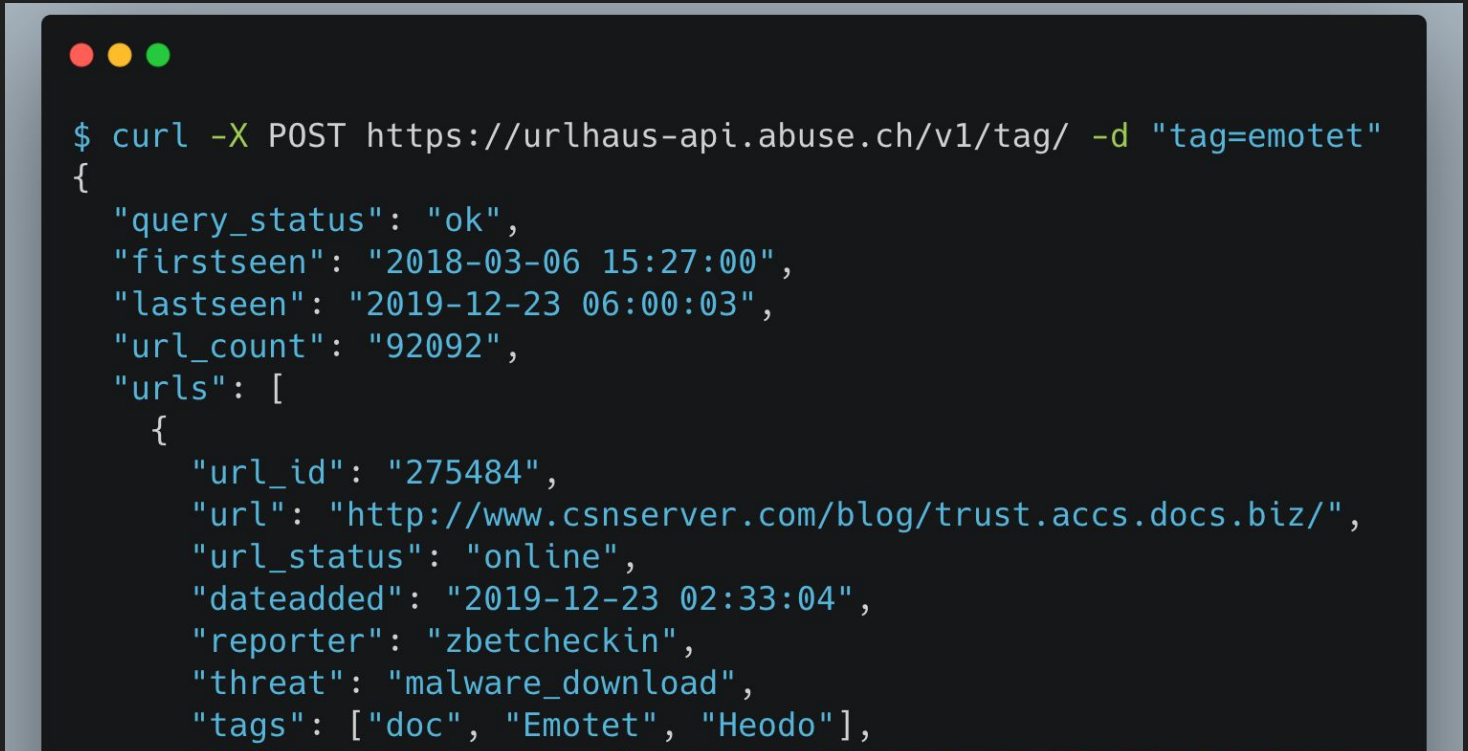
- URLhaus: https://urlhaus.abuse.ch/
  - Malware URL exchange by abuse.ch.
  - 情報源:
    - abuse.ch, 個人によるレポート, etc.
- IOC-DB: https://labs.inquest.net/iocdb
  - Indicator of Compromise database by InQuest.
  - 情報源:
    - Twitter, GitHub and blogs.
- Twitter IOC Hunter: http://tweettioc.com/#
  - Twitter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



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.csnserver.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"],
```

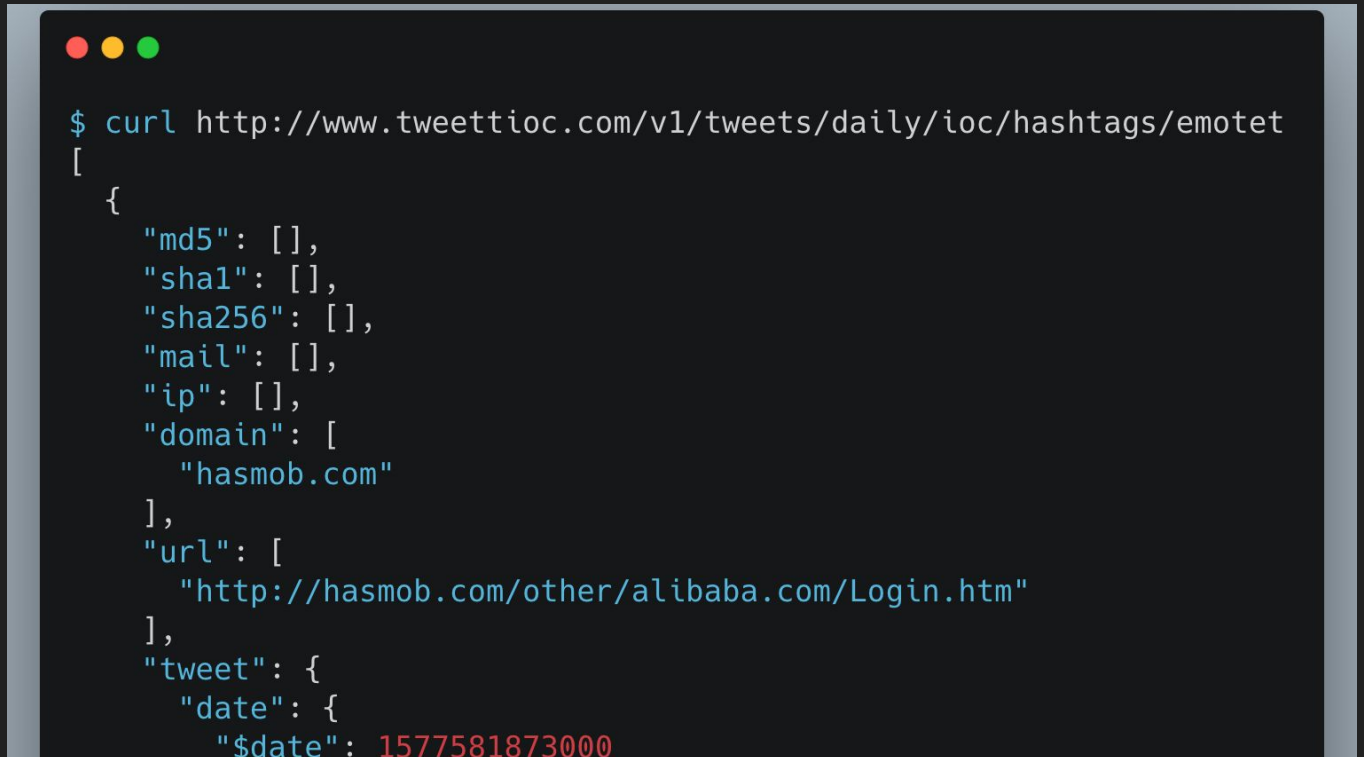
Emotet IoC Feeds

- 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 =
\"Detects Emotet JS dropper\"\n      author = \"Florian Roth\"\n      reference =
\"https://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

https://twitter.com/plusvic/status/778983467627479040?s=20

Where can we use YARA?

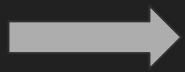
- オンラインサービス
  - Hybrid Analysis
    - https://www.hybrid-analysis.com/
  - VirusTotal Hunting
    - https://www.virustotal.com/gui/hunting-overview
  - Malpedia
    - https://malpedia.caad.fkie.fraunhofer.de/ (Invitation only)
  - Koodous
    - https://koodous.com/ (Android malware only)
- YARA command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


YARA:
MoqHao

Fake Sagawa Express Mobile Application (MoqHao)

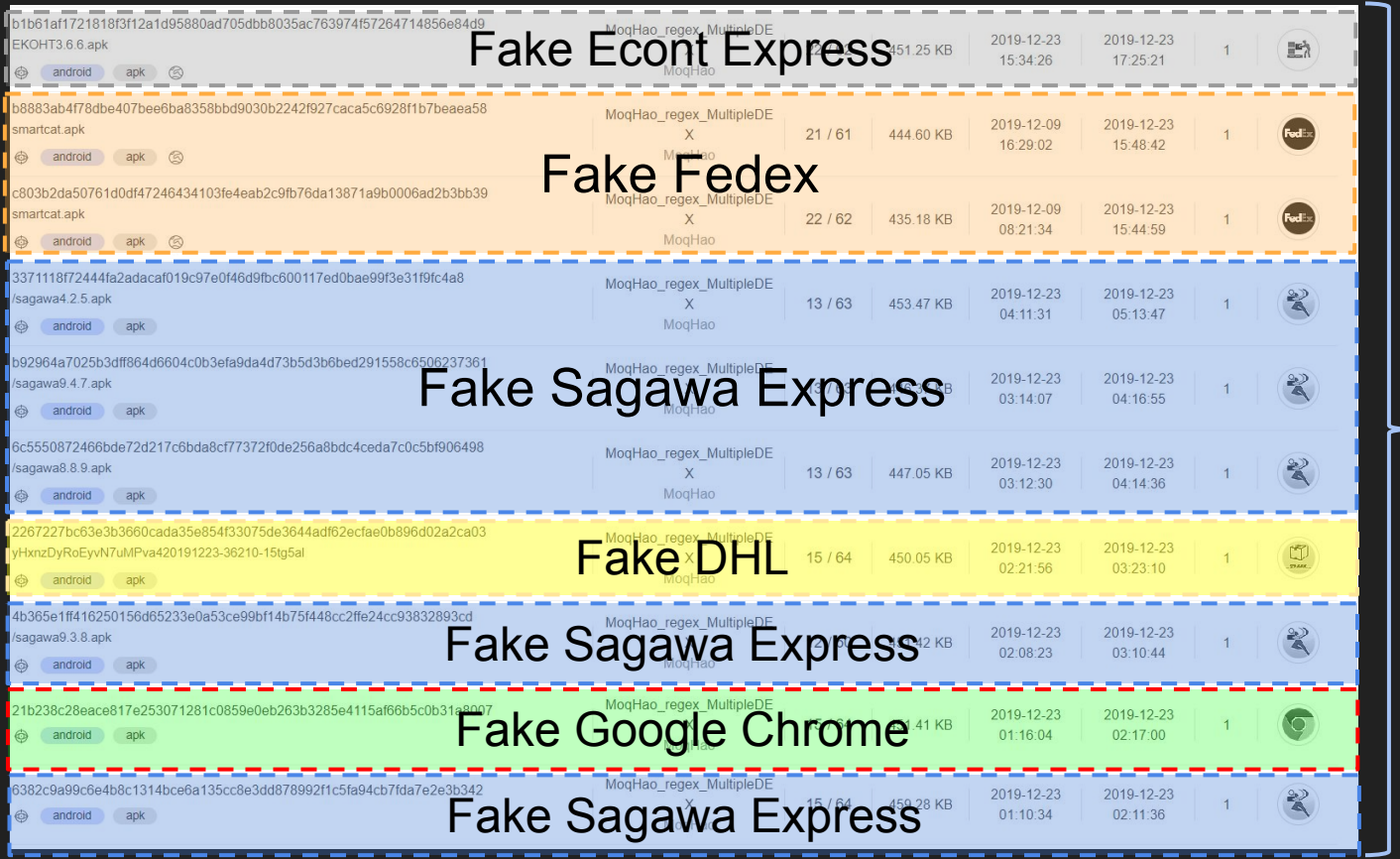
- 佐川急便に偽装したAndroidマルウェア
- MoqHaoを検知するためのYARAルール

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

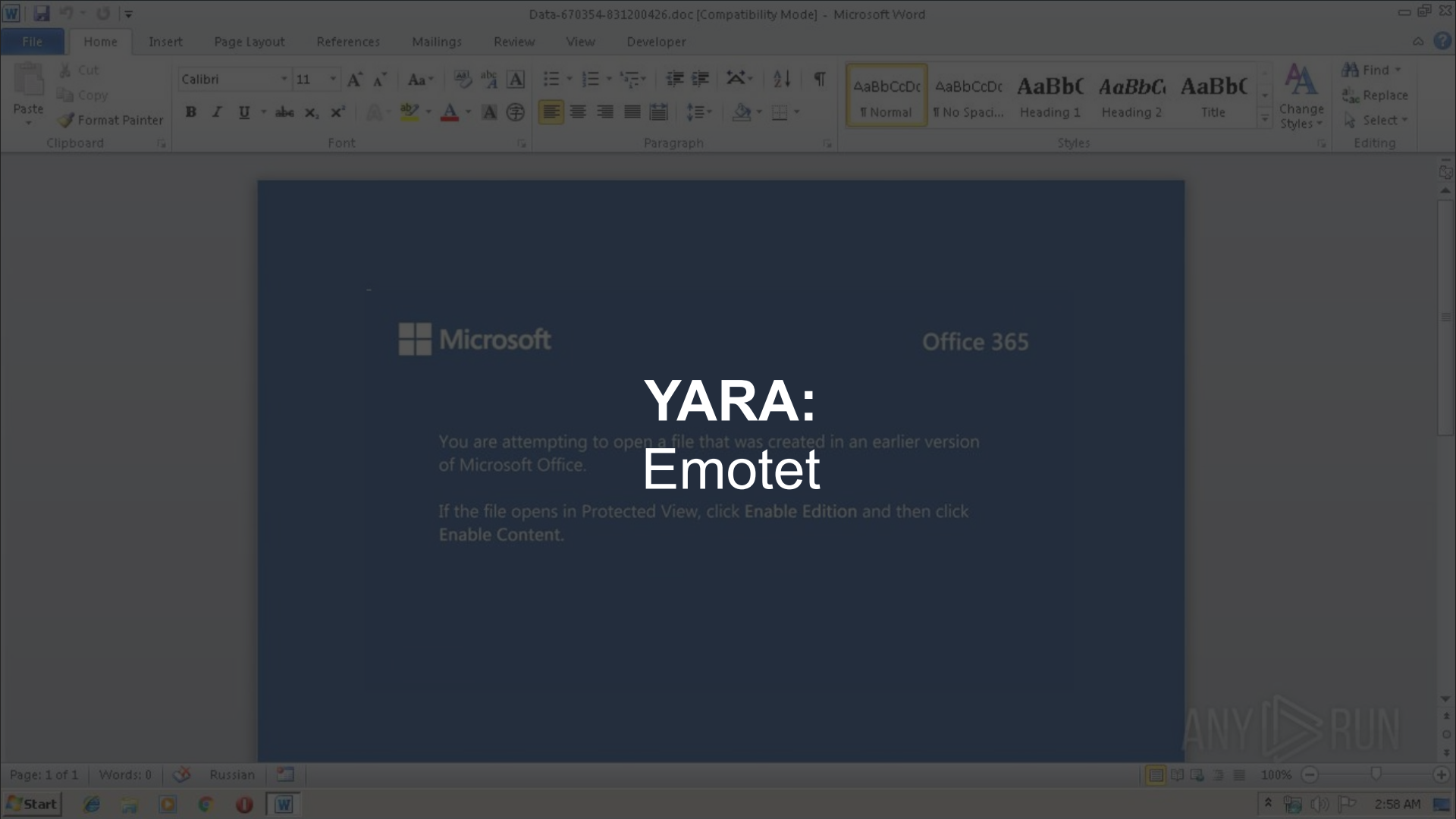


VT hunting
に登録

Results of VT Hunting with a YARA rule for MoqHao

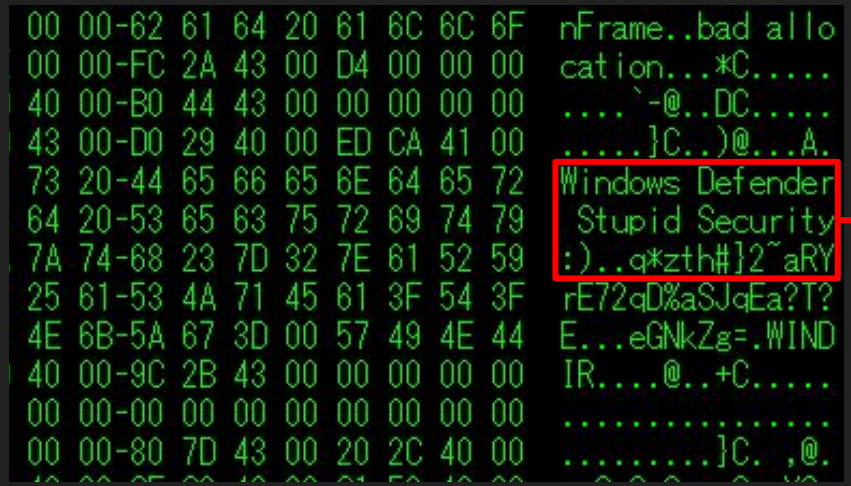


佐川急便以外の亜種のMoqHaoも自動的に捕捉することができる

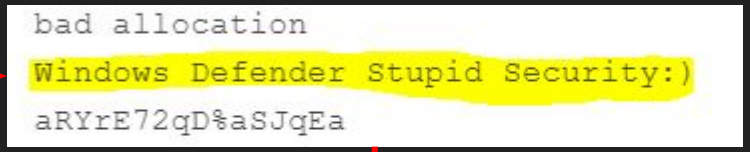

Data-670354-831200426.doc [Compatibility Mode] - Microsoft Word
File
Home
Insert
Page Layout
References
Mailings
Review
View
Developer
Microsoft
Office 365
You are attempting to open a file that was created in an earlier version of Microsoft Office.
If the file opens in Protected View, click Enable Edition and then click Enable Content.
YARA:
Emotet
Page: 1 of 1
Words: 0
Russian
2:58 AM

Emotet

- 特徴的な文字列がEmotetの中にある



MD5:f8105a0e4af7d61006e5e3974710daf3

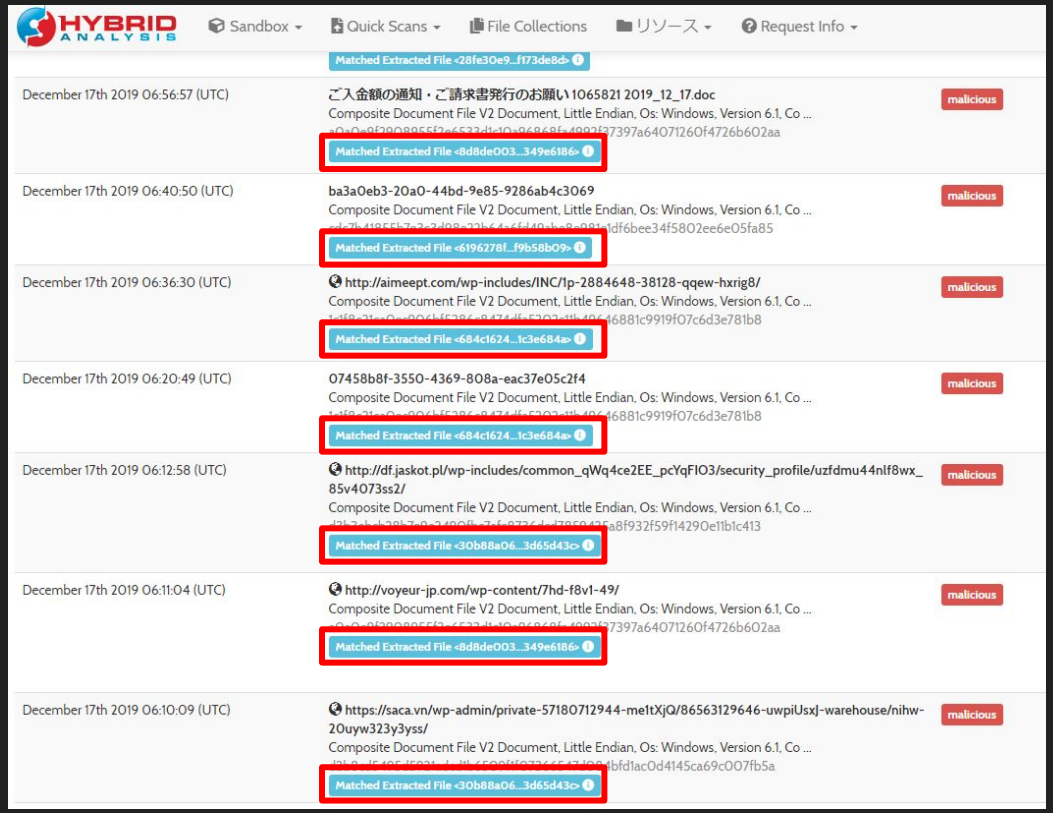


この文字列をベースにYARAルールを作成

```
rule emotet
{
    meta:
        date = "2019-12-17"
        Family = "Emotet"
    strings:
        $a = "Windows Defender Stupid Security"
    condition:
        (uint16(0) == 0x5A4D)
        and $a
}
```

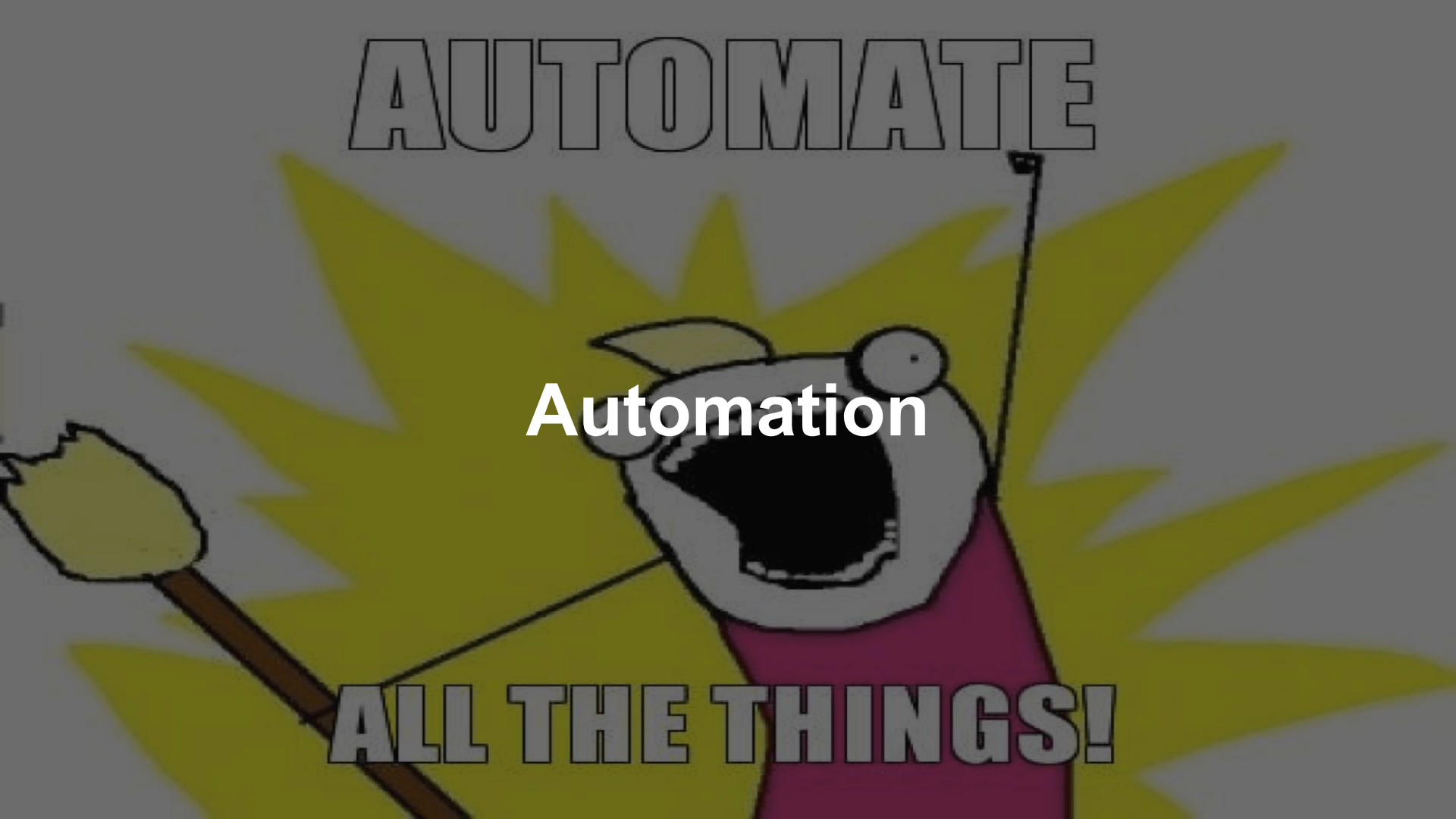
このYARAルールでEmotetを捕捉してみよう

Search result of Hybrid Analysis with YARA rule for Emotet



Considerations:

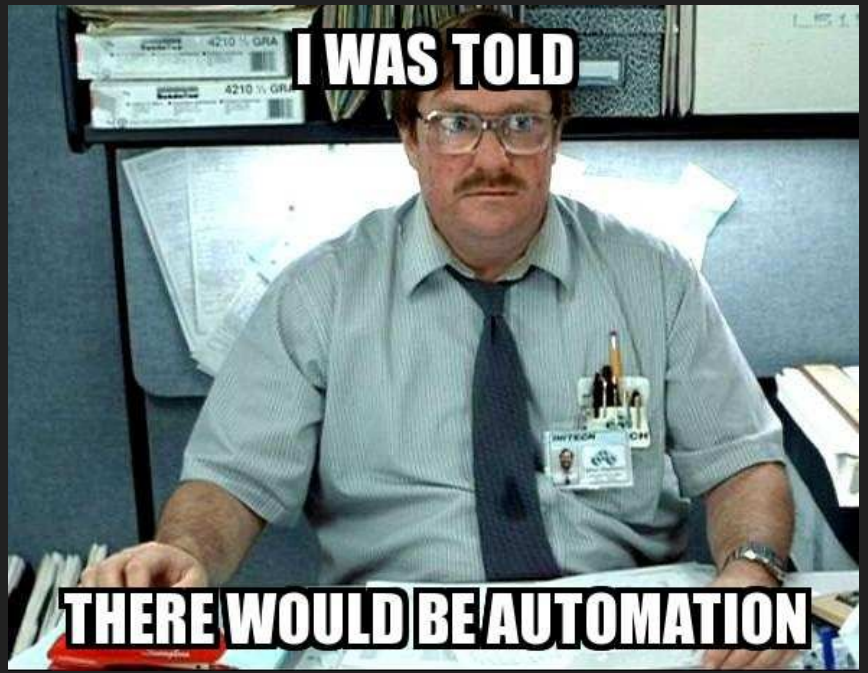
- Hybrid Analysisには38個のサンプルがあり、2019/12/16から2019/12/17にかけて使用されていた



Automation

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

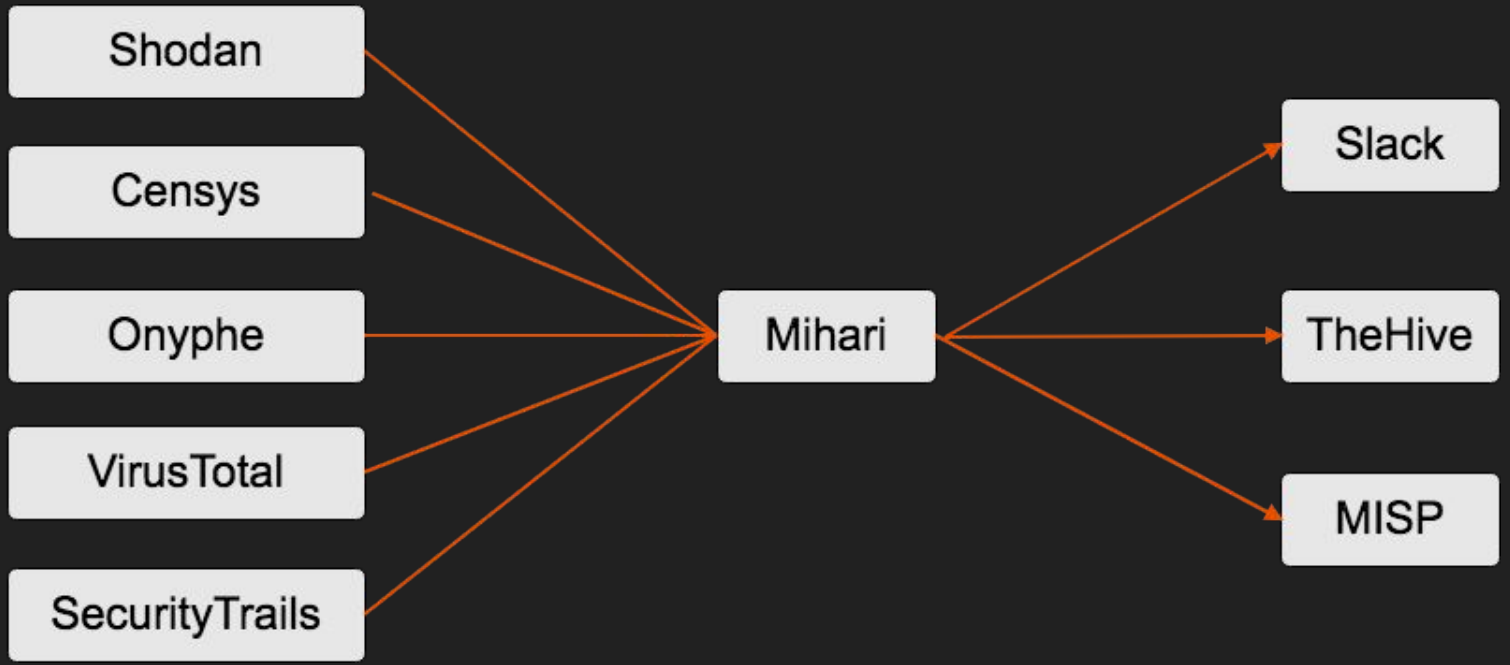
- Apullo:
  - ネットワーク関連のフィンガープリントを取得するためのツール
  - https://github.com/ninoseki/apullo
- Mihari:
  - Shodan, Censys, BinaryEdge等を活用したモニタリングツール
  - https://github.com/ninoseki/mihari
- InQuest/ThreatIngestor:
  - IoCを抽出し、集約するためのツール
  - https://github.com/InQuest/ThreatIngestor

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

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

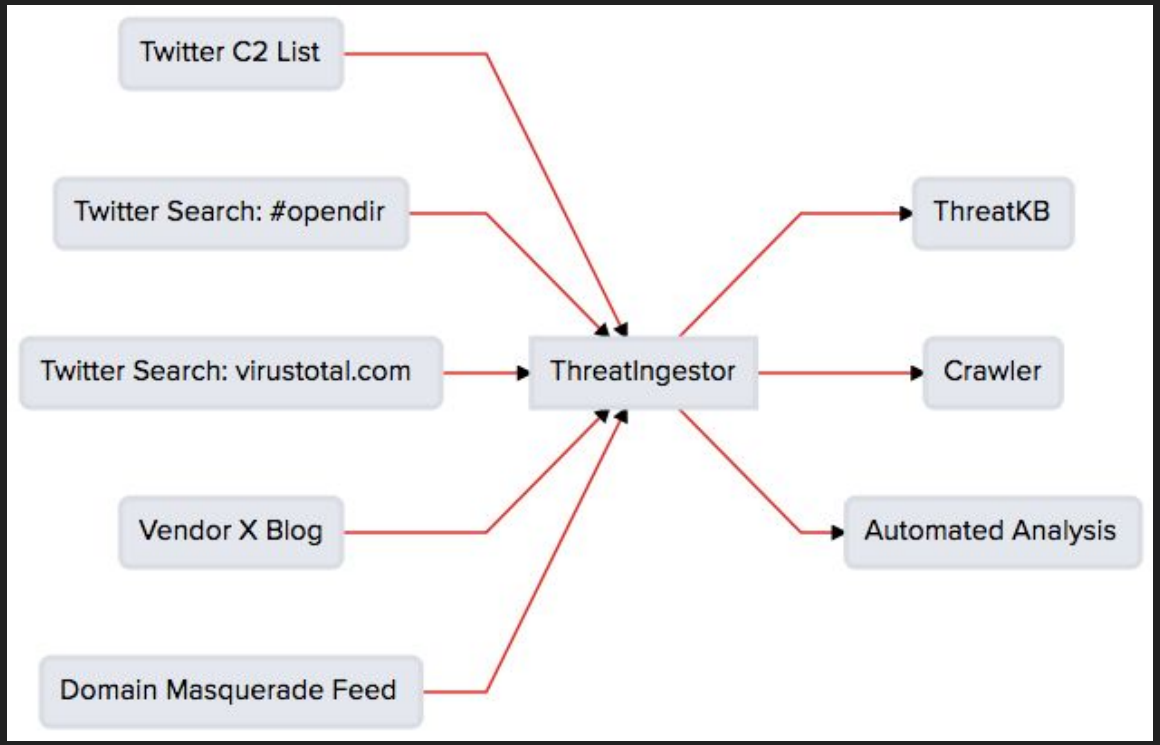


Mihari

- 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

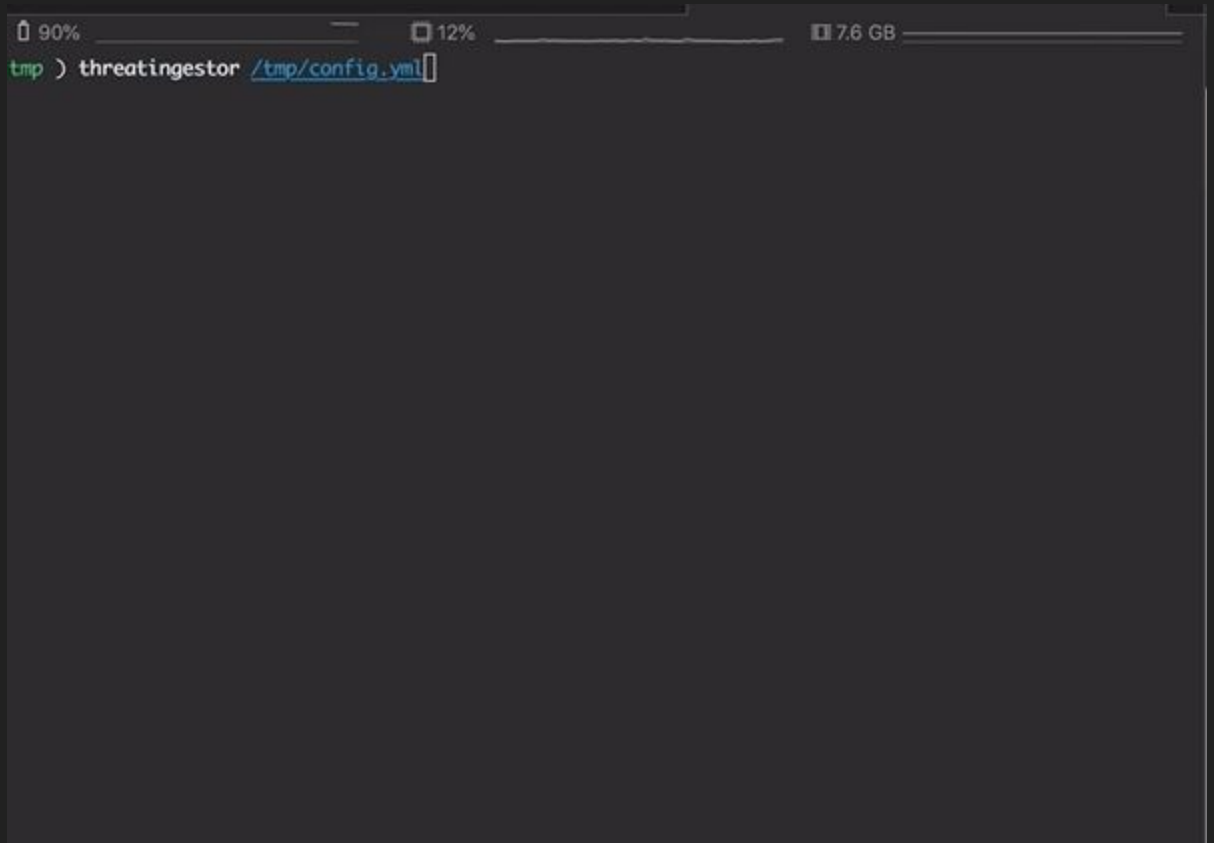
- InQuestのIOC-DBを支えるデーモン



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



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

List: Tools/Services

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