100 more behind cockroaches?

or how to hunt IoCs with OSINT

Hiroaki Ogawa & Manabu Niseki

Before Starting

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

“For every cockroach you see there are 100 more behind the walls”

Does it apply to cyber threats?

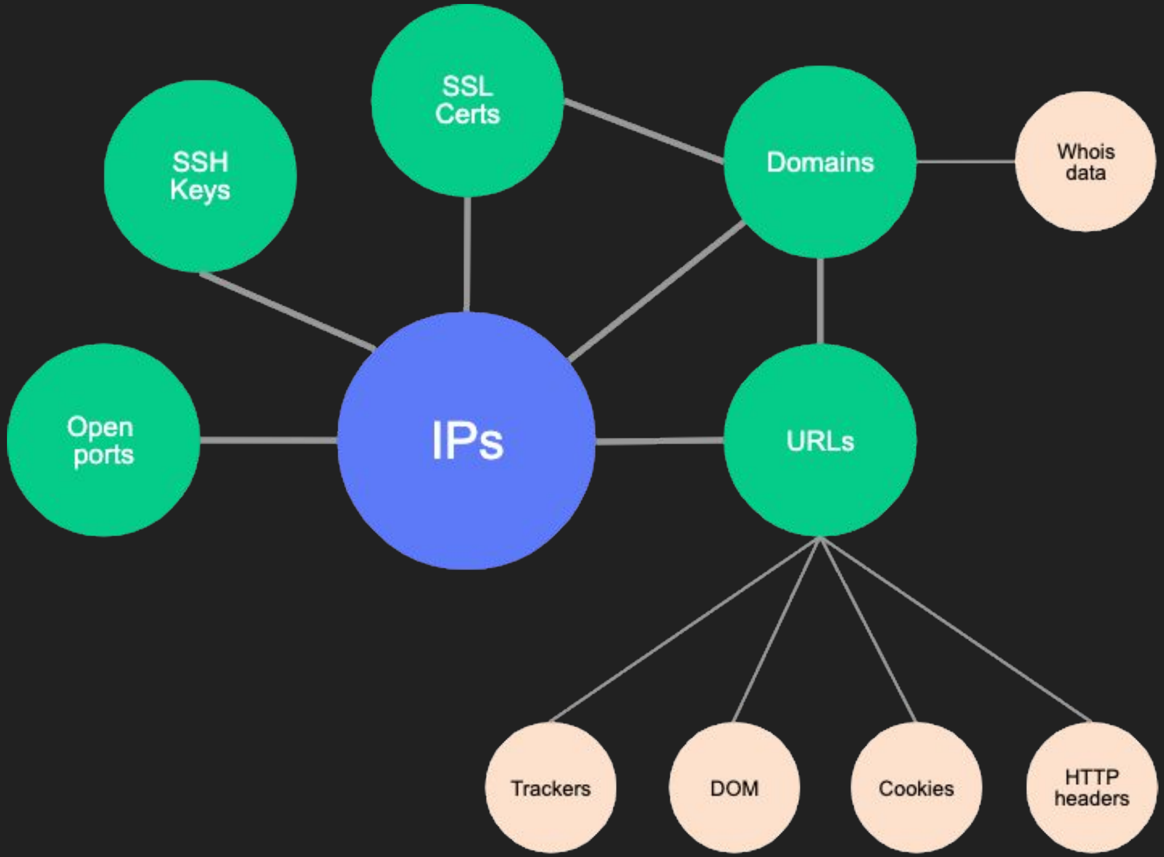
YES

We have to install traps!

Tracking Fingerprints

- Attackers are good friends with bad habits.
  - Reusing infrastructures
  - Reusing components
  - Reusing SSL certificates
  - Reusing SSH host keys
- Reusing something increases a possibility of tracking.
  - Let’s say it's a fingerprint of an attacker.
  - You can track him down based on his fingerprint.

Fingerprints on the Internet



Methodologies

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

Domain Fuzzing

Domain Fuzzing

- Techniques to find typosquatting domains.
  - Converting **1** to **2** or **q**. (See your QWERTY keyboard)
  - Converting **a** to **à**, **á**, **â**, **ã**, **ä**, **å**, **ɑ**, **ạ**, **ǎ**, **ă**, **ȧ** or **ą**.
  - Converting a vowel(**a, e, i, o** or **u**) to another vowel.
    - e.g. example.com
      - **a**xample.com, **i**xample.com, **o**xample.com, **u**xample.com, ...
  - etc.
- Domain fuzzing is useful for finding similar domains.

Domain Fuzzing:

MoqHao

MoqHao

- An Android malware.
- It uses DGA like domains.

ysu3g.xyz

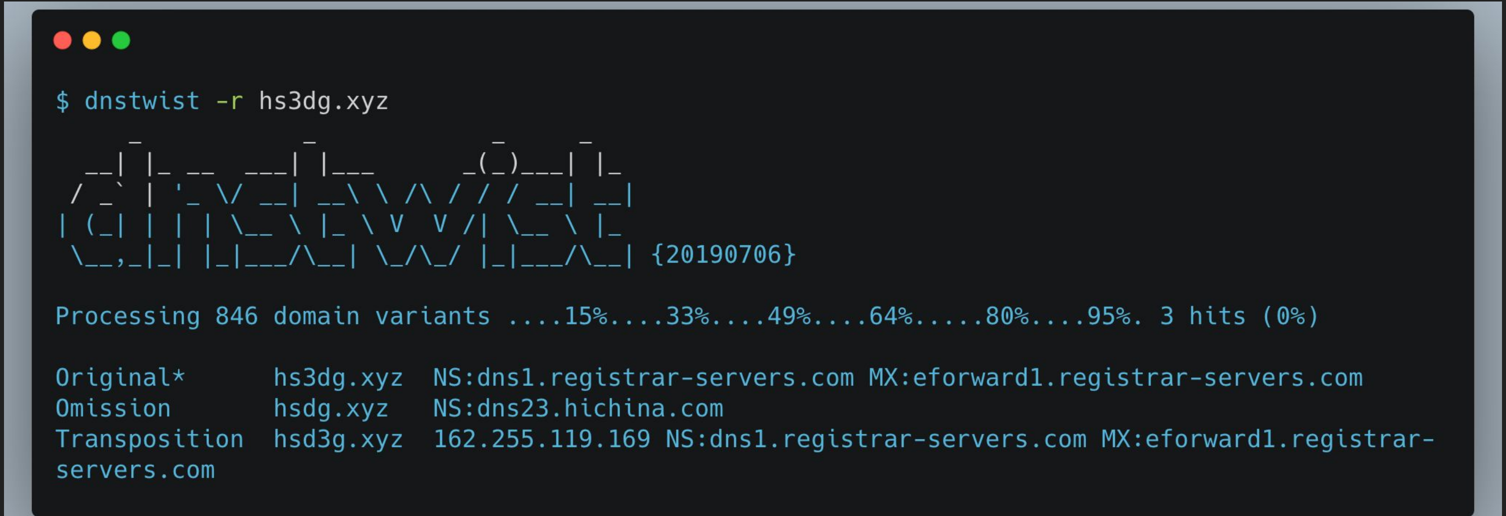
hs3dg.xyz

Nsi3h.xyz

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

MoqHao

- How to do domain fuzzing for finding MoqHao hosts.
  - Write your own script. 😉
    - https://gist.github.com/ninoseki/8c3b9dd54506691c105c629cd3aa284e
  - Use dnstwist.
    - https://github.com/elceef/dnstwist



```
$ dnstwist -r hs3dg.xyz
     _           _            _     _
  __| |_ __  ___| |___      _(_)___| |_
 / _` | '_ \/ __| __\ \ /\ / / / __| __|
| (_| | | | \__ \ |_ \ V  V /| \__ \ |_
 \__,_|_| |_|___/\__| \_/\_/ |_|___/\__| {20190706}

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
```

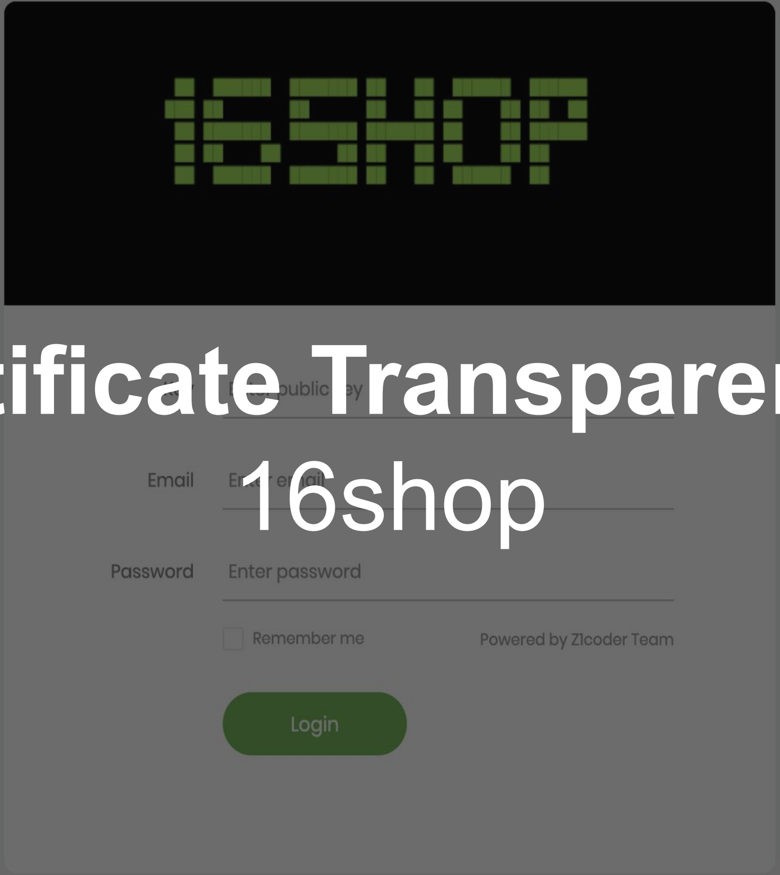
Certificate Transparency

Certificate Transparency

- Certificate Transparency enables to monitor HTTPS websites.
    - http://www.certificate-transparency.org/
    - Roughly speaking, Certificate Transparency gives you newly domains for free.
- Useful services/tools:
    - 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

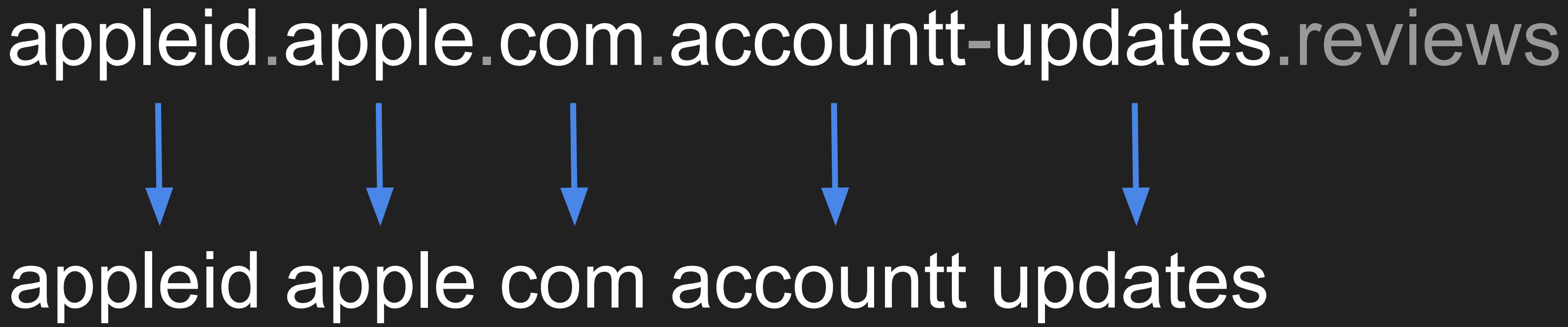
- An Indonesian phishing kit targeting Apple and Amazon users.
  - Akamai says 16shop is “a highly sophisticated phishing kit.”.
    - https://blogs.akamai.com/sitr/2019/05/16shop-commercial-phishing-kit-has-a-hidden-backdoor.html
  - C2:
    - 128.199.154.155 / 167.99.79.91

16shop

- Does 16shop use HTTPS?
    - 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

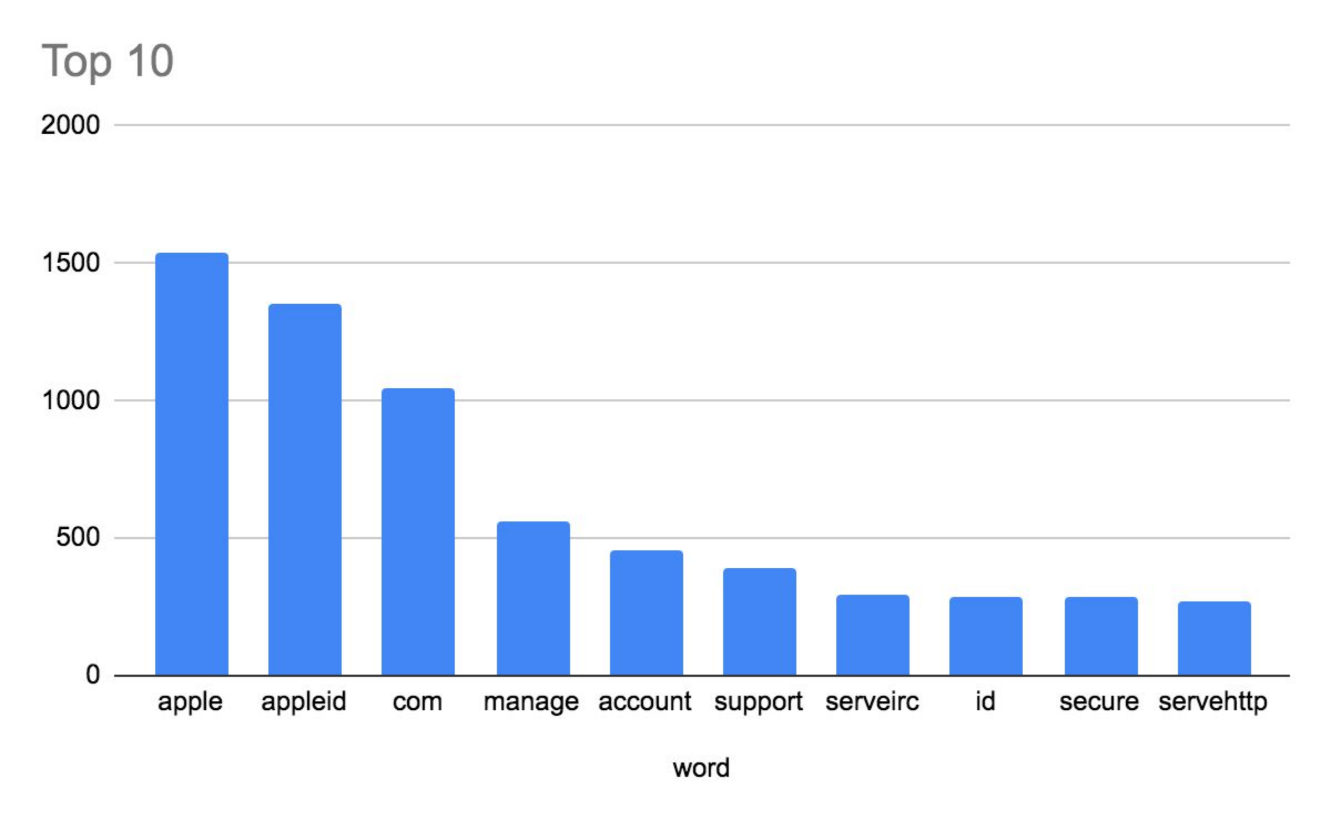
- Analyzing occurrences of words in 6,500+ 16shop domains.



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

- If a CN in a CT log contains common 16shop words, it might be a 16shop website.
- You can check whether it is 16shop or not by checking an HTTP response hash of **/admin/index.php**
  - 16shop Apple version.
    - 0e06d02dab03e8085b18ebedb0f54dc68508c40c5d1b8c6e3e8da98e3d3b6649
    - ce4fe392dd0f996923c5cf272d98e1e2778a2a44ffb2a4435fdb9c13665215f3
  - 16shop Amazon version.
    - 2edfff035a357aec4cea23057ea2e10af1dd3431713c904cf1cd804640bd2965

Omake: Bizarre Domains

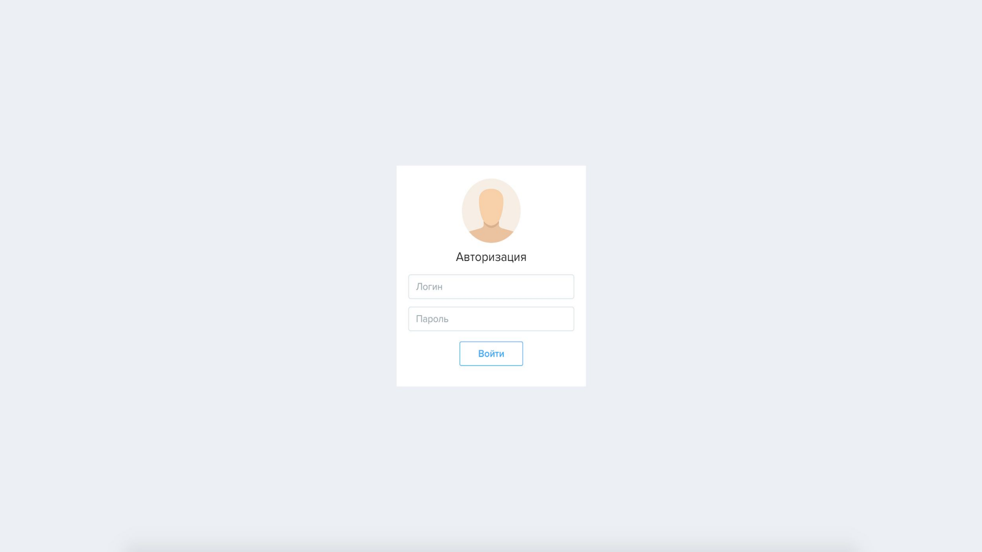
- manage.unauthorized.login.amazon.co.jp.omachikudasai.com
- xn--id-zb4axila5esc1e1f9bvhzd4a6fe.manage-konohajp.tokyo(アップルジャパンのログインid.manage-konohajp.tokyo)
- youji-kyoiku.com

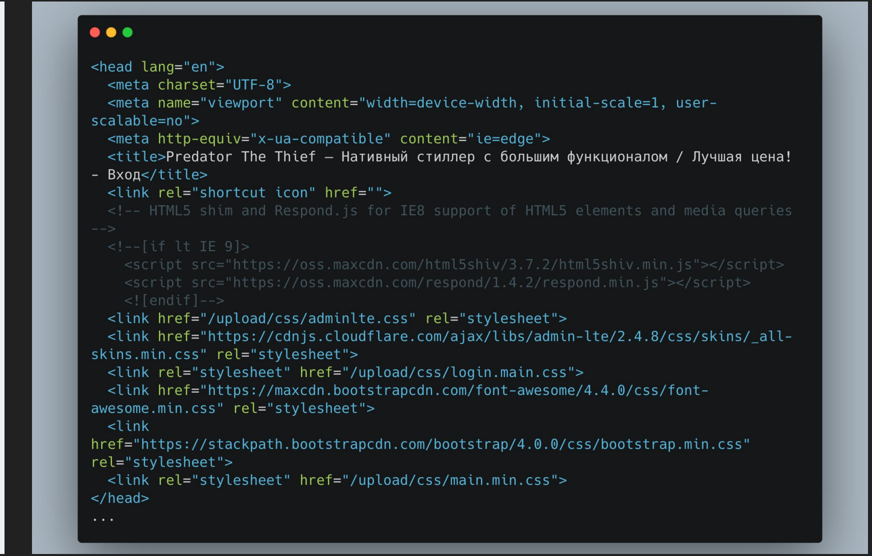
HTTP fingerprint

HTTP Fingerprint:
Predator The Thief

Predator The Thief

- A stealer malware.
- @fumik0_ published a detailed report about Predator The Thief.
  - https://fumik0.com/2018/10/15/predator-the-thief-in-depth-analysis-v2-3-5/
- Predator The Thief C2 returns a static HTTP response.





```
<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

- “A static HTTP response” means it always returns same HTTP response.
  - It can be used as a fingerprint.
- Queries for Predator The Thief C2:
  - Censys(SHA256):
    - b064187ebdc51721708ad98cd89dacc346017cb0fb0457d530032d387f1ff20e
  - BinaryEdge(SHA256):
    - b064187ebdc51721708ad98cd89dacc346017cb0fb0457d530032d387f1ff20e
  - Shodan(MurmurHash3):
    - http.html_hash:-1467534799

HTTP Fingerprint:
PANDA

PANDA

U Name…

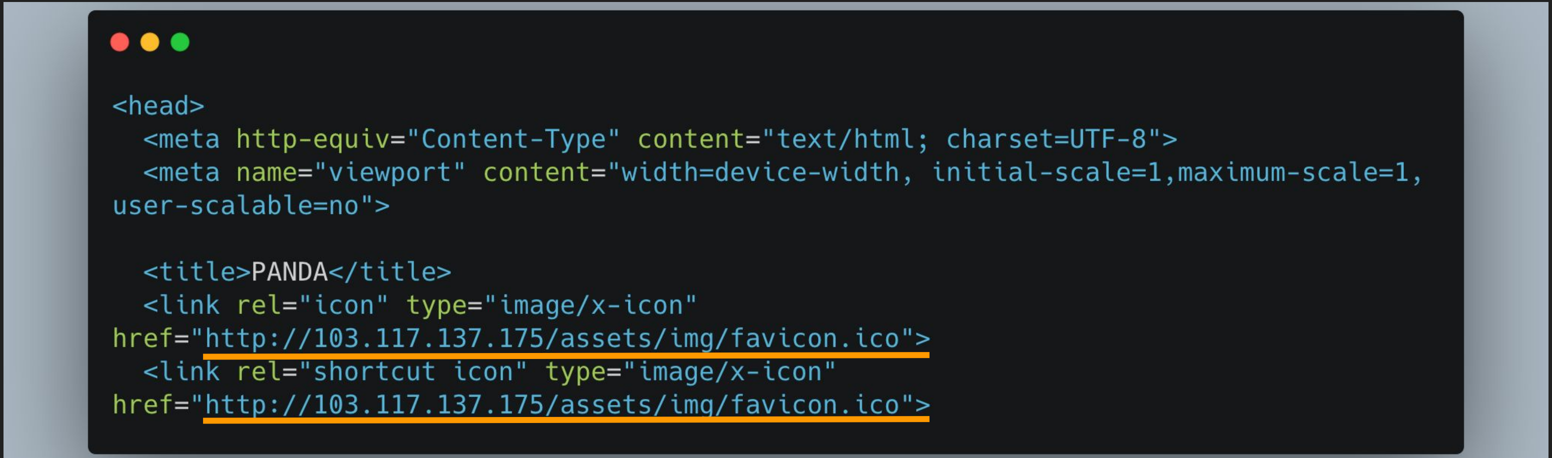
P Password…

□ Remember me

copyright @2018 [illegible]min

PANDA

- PANDA is used by ShadowVoice.
  - FSI published a report about ShadowVoice in BlackHat Asia 2019.
  - https://i.blackhat.com/asia-19/Fri-March-29/bh-asia-Jang-When-Voice-Phishing-Met-Malicious-Android-App-updated.pdf
- HTTP response of PANDA is not static.
  - Because it uses an absolute path to load a resource.



```
<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">
```

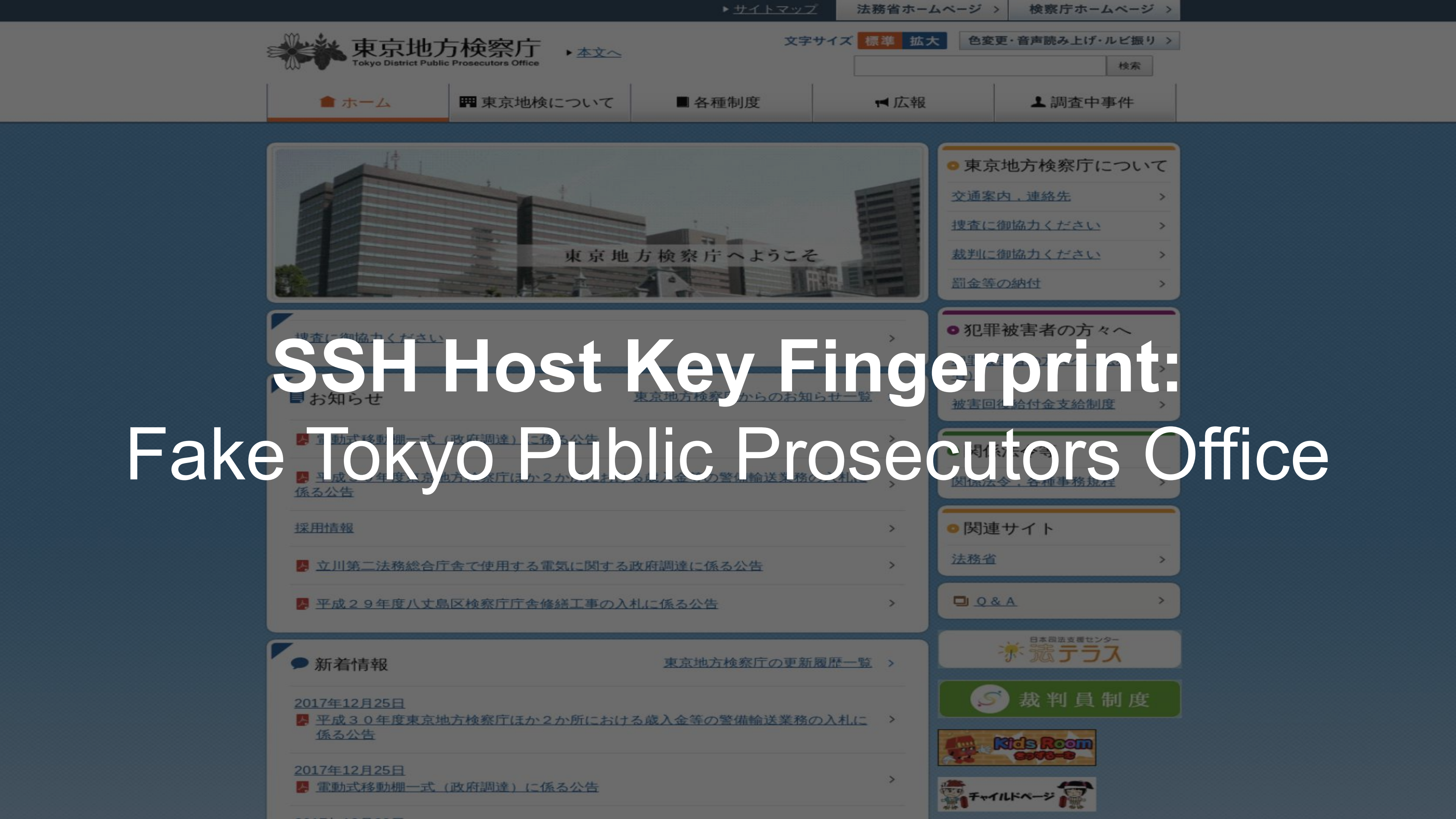
PANDA

- So the hash value matching doesn’t work.
- Instead of the hash value matching, you can use another techniques.
  - Free text, favicon hash, etc.
- Queries for PANDA C2:
  - 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



▸ サイトマップ 法務省ホームページ ＞ 検察庁ホームページ ＞

東京地方検察庁
Tokyo District Public Prosecutors Office

▸ 本文へ

文字サイズ 標準 拡大 色変更・音声読み上げ・ルビ振り ＞

検索

ホーム | 東京地検について | 各種制度 | 広報 | 調査中事件

東京地方検察庁へようこそ

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

電動式移動棚一式（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
電動式移動棚一式（政府調達）に係る公告 ＞

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 ＞

関係法令，各種事務規程 ＞

関連サイト

法務省 ＞

Q & A ＞

日本司法支援センター 法テラス

裁判員制度

Kids Room

チャイルドページ

Fake Tokyo Public Prosecutors Office

- A scam impersonating the Tokyo Public Prosecutors Office.
  - A kind of fraud.
- Hosts of fake websites reuse same SSH host key.
- Queries for fake hosts:
  - 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

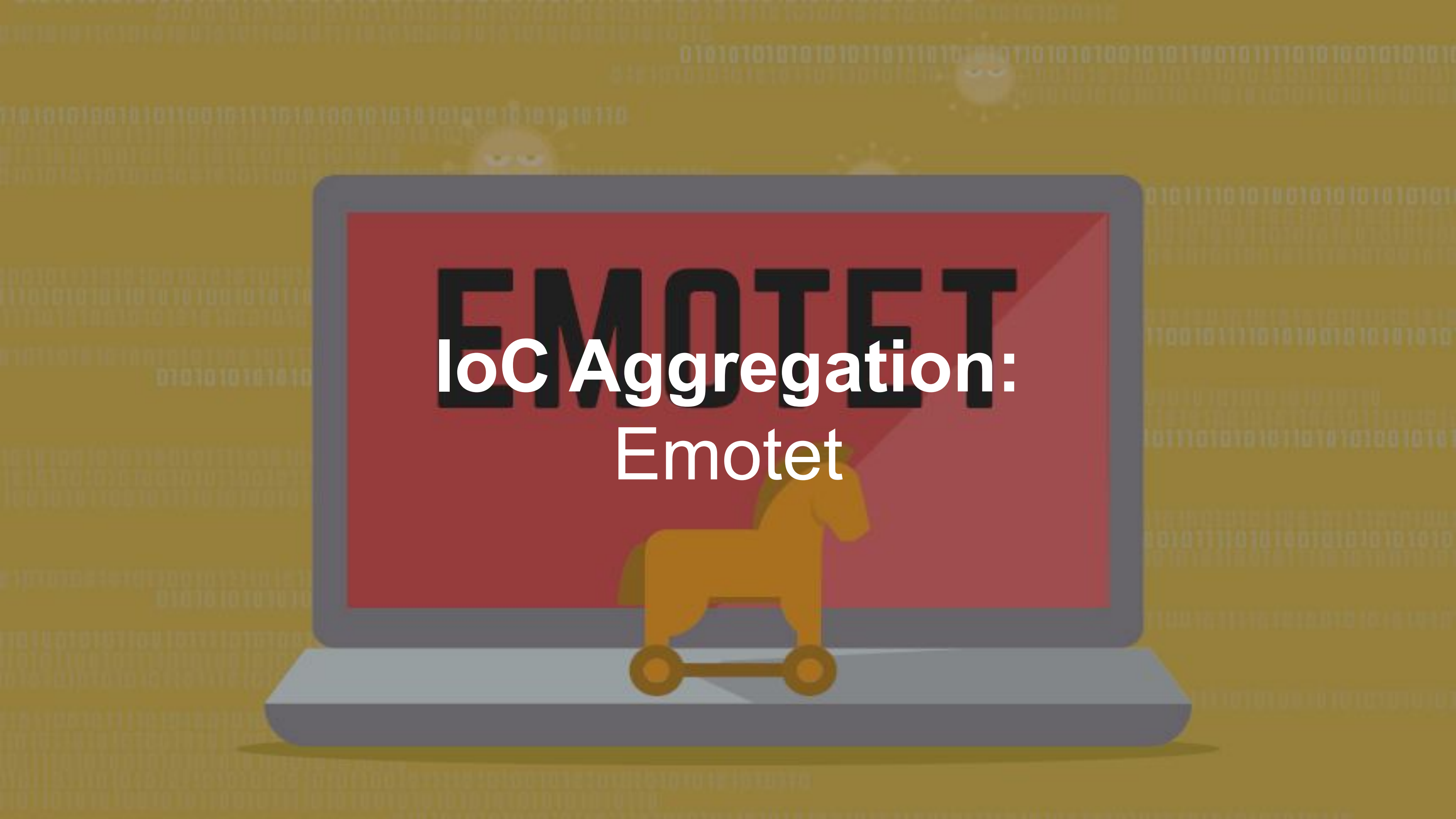
IoC Feeds Aggregation

IoC Feeds

- URLhaus: https://urlhaus.abuse.ch/
    - Malware URL exchange by abuse.ch.
    - Sources:
        - abuse.ch, individuals, etc.
- IOC-DB: https://labs.inquest.net/iocdb
    - Indicator of Compromise database by InQuest.
    - Sources:
        - Twitter, GitHub and blogs.
- Twitter IOC Hunter: http://tweettioc.com/#
    - Twitter based IoC database/feed by @fatihsirinnnn.
    - Sources:
        - Twitter

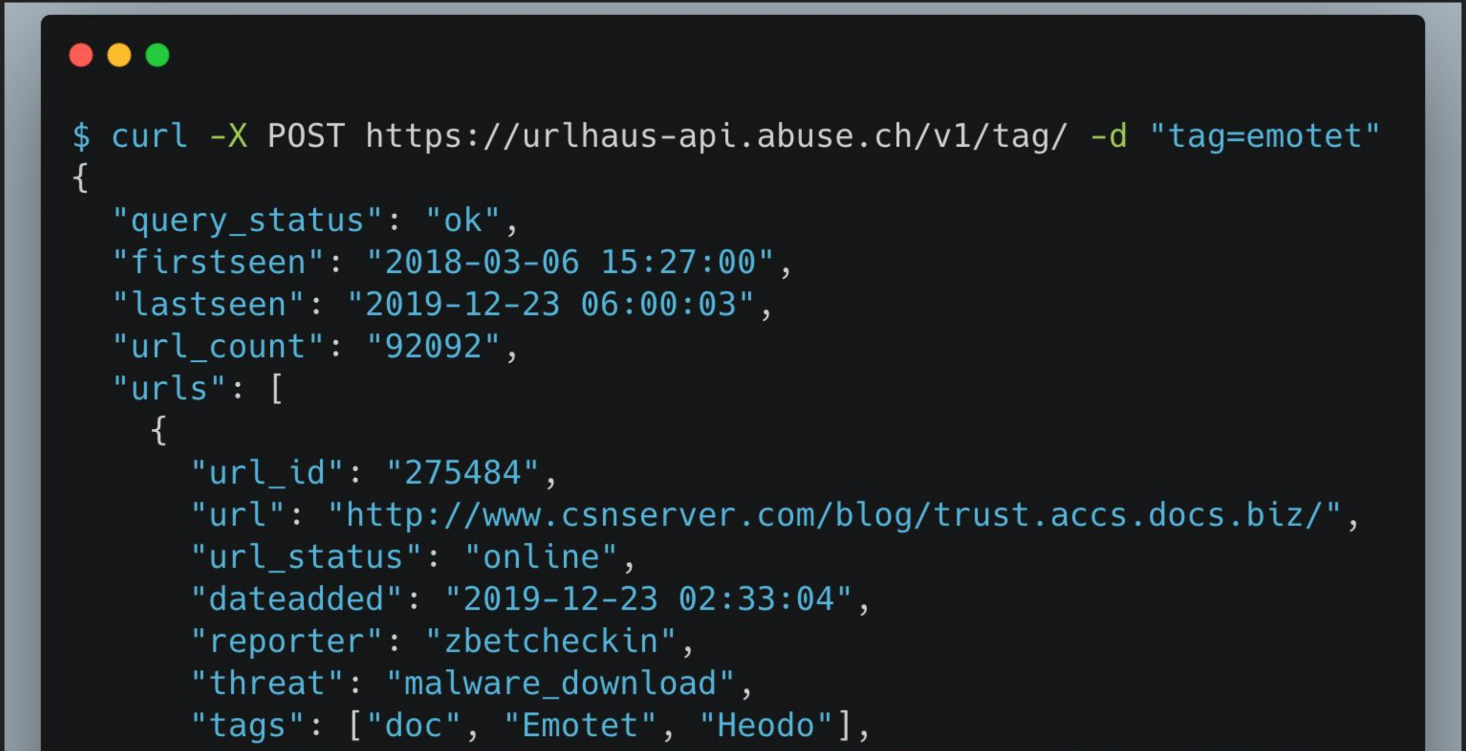
IoC Aggregation:

Emotet



Emotet IoC Feeds

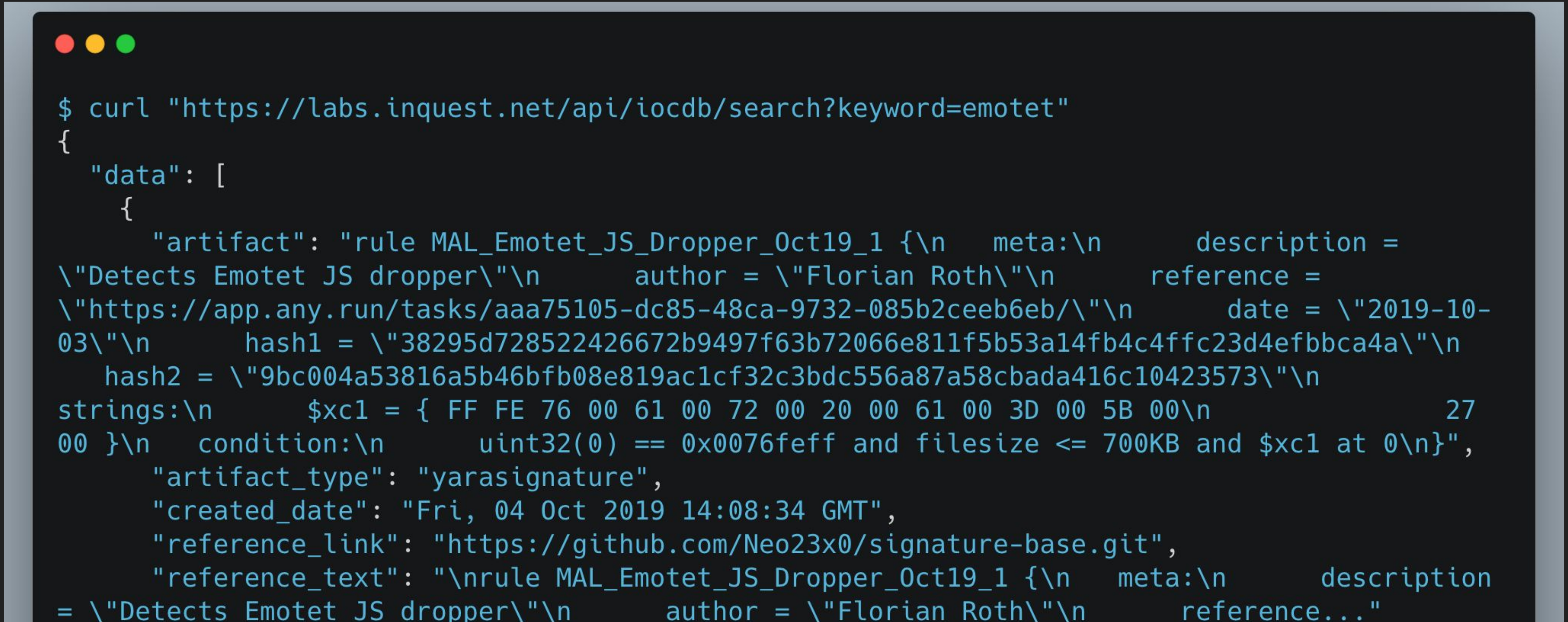
- URLhaus:



```
$ 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

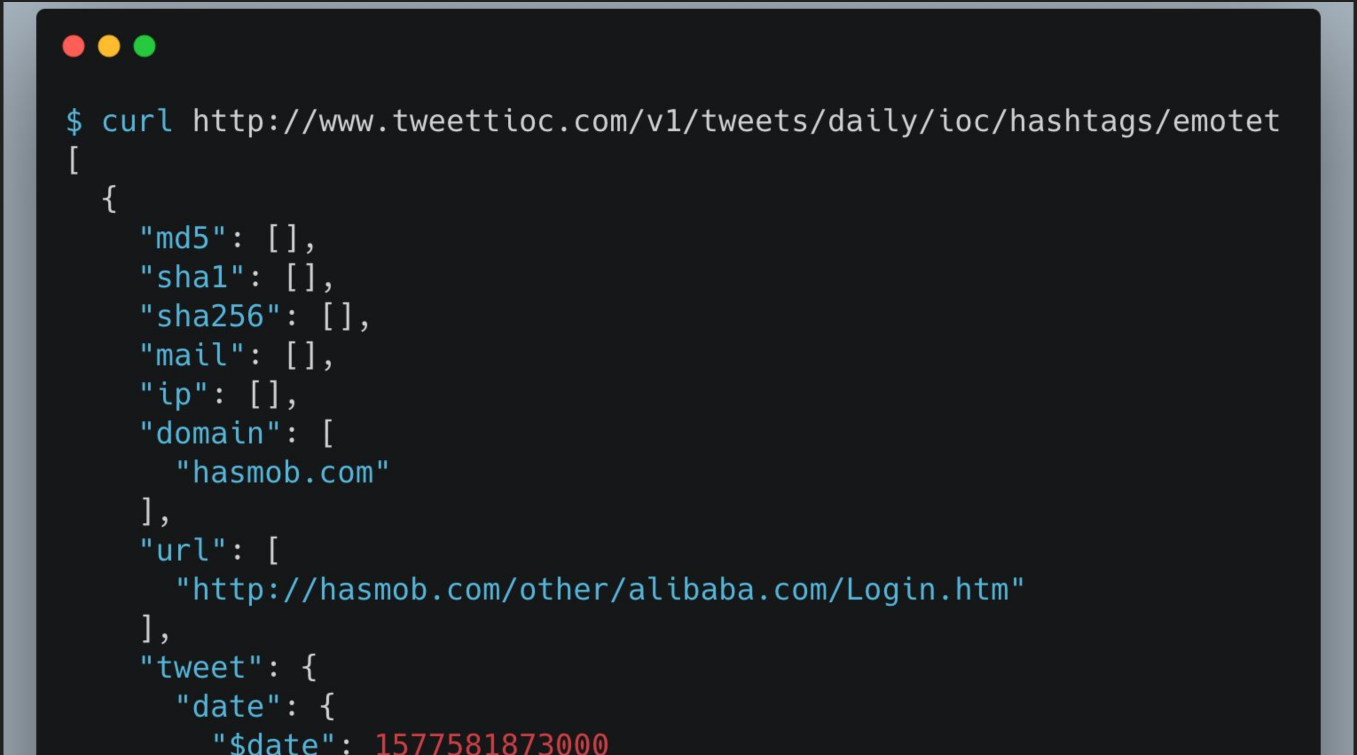
- IOC-DB:



```
$ 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:

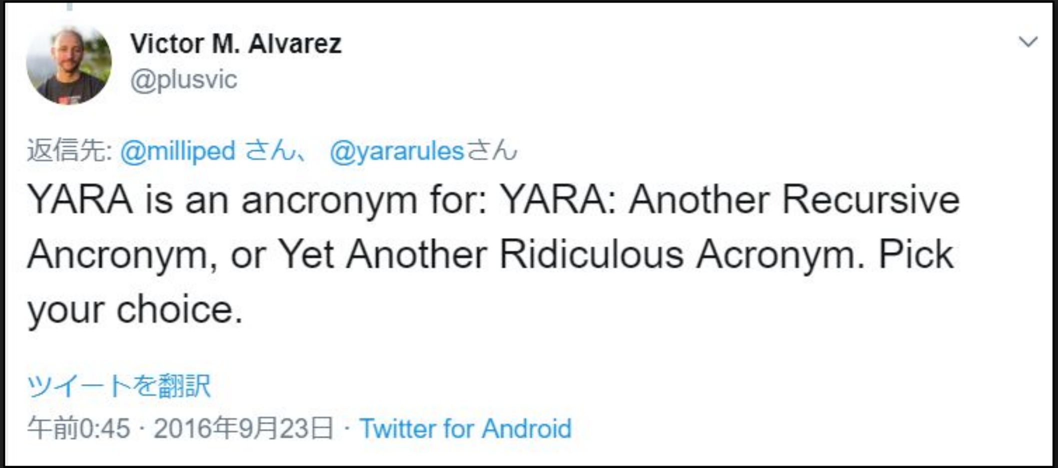


```
$ curl http://www.tweettioc.com/v1/tweets/daily/ioc/hashtags/emotet
[
  {
    "md5": [],
    "sha1": [],
    "sha256": [],
    "mail": [],
    "ip": [],
    "domain": [
      "hasmob.com"
    ],
    "url": [
      "http://hasmob.com/other/alibaba.com/Login.htm"
    ],
    "tweet": {
      "date":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

YARA

YARA

- YARA is a tool aimed at helping malware researchers to identify and classify malware samples.
- With YARA, it could catch files that has same strings or binaries from a large number of files and could be grouping these files.



Victor M. Alvarez
@plusvic

返信先: @milliped さん、 @yararulesさん

YARA is an ancronym for: YARA: Another Recursive Ancronym, or Yet Another Ridiculous Acronym. Pick your choice.

ツイートを翻訳

午前0:45 · 2016年9月23日 · Twitter for Android

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

Where can we use YARA?

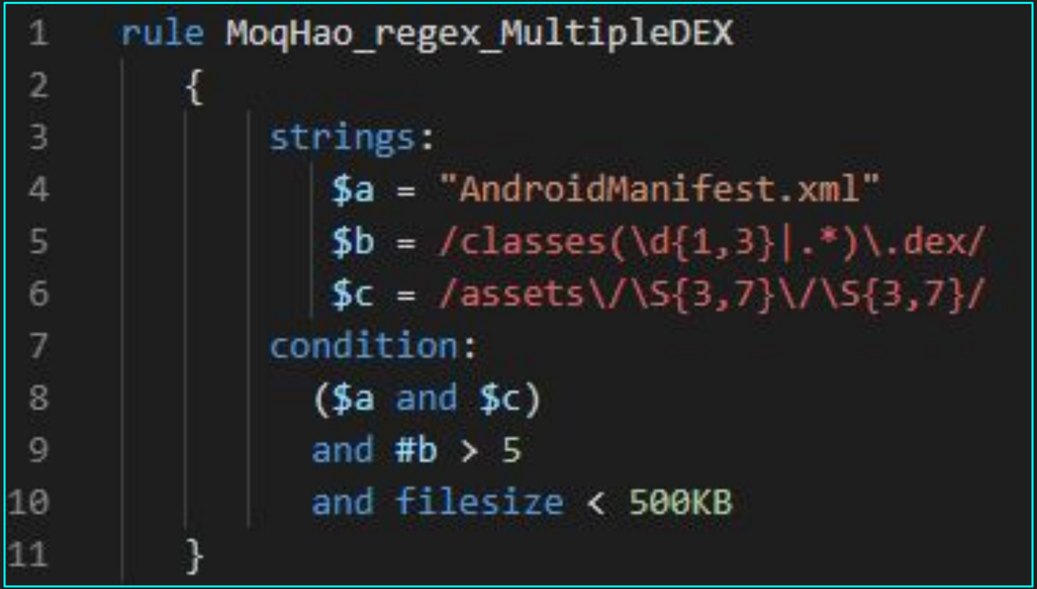
- Online services
  - Hybrid Analysis
    - https://www.hybrid-analysis.com/
  - VirusTotal Hunting
    - https://www.virustotal.com/gui/hunting-overview
  - Malpedia
    - https://malpedia.caad.fkie.fraunhofer.de/ (Invitation only)
  - Koodous
    - https://koodous.com/ (Android malware only)
- YARA command line tool
    - https://virustotal.github.io/yara/

YARA:

MoqHao

Fake Sagawa Express Mobile Application (MoqHao)

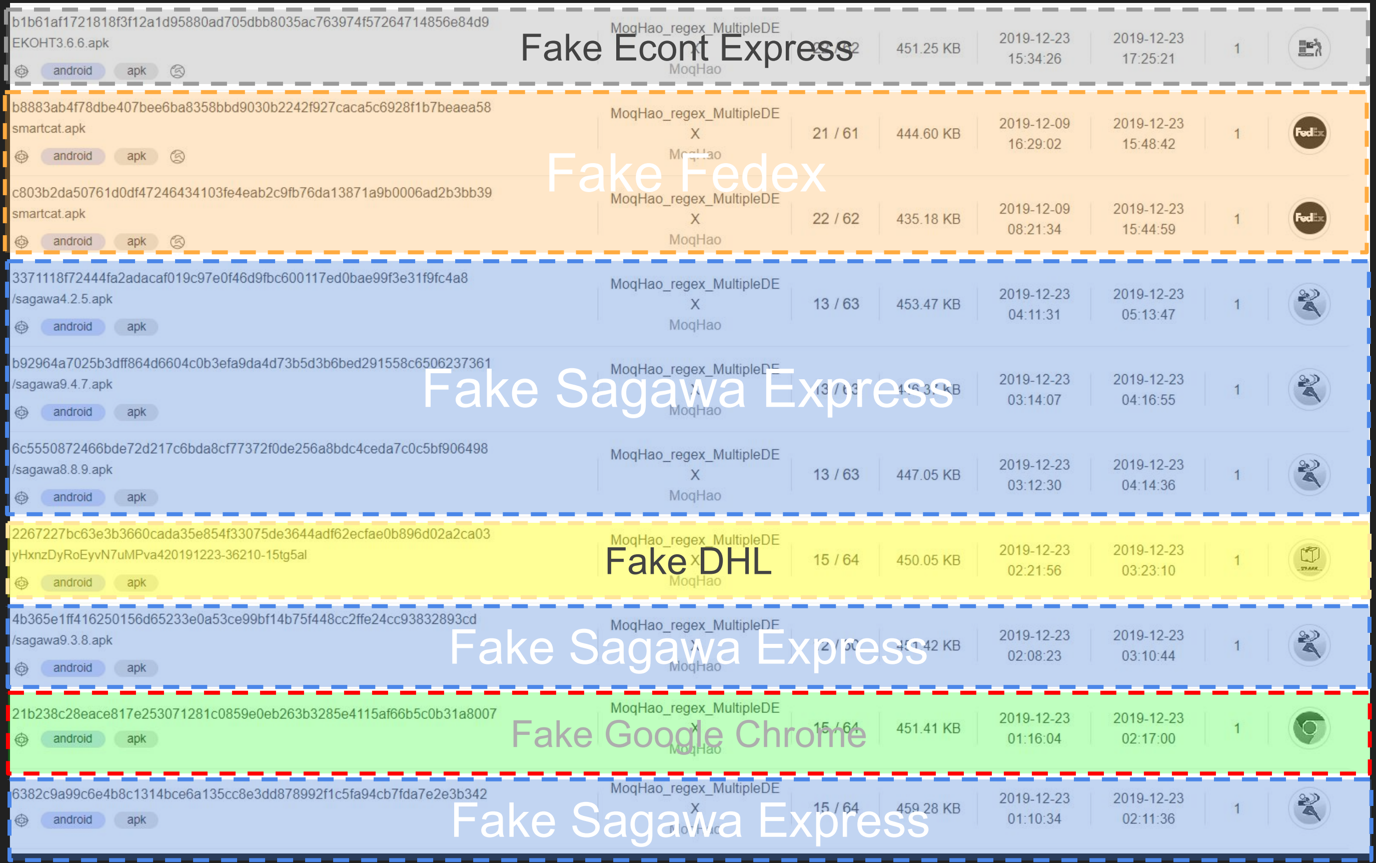
- Fake mobile app is used in a SMiShing campaign which impersonates Sagawa Express. The fake mobile app is malware called MoqHao.
- Here is a YARA rule for fake Sagawa Express mobile app.



```
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
    }
```

Set it to the VT hunting

Results of VT Hunting with a YARA rule for MoqHao



b1b61af1721818f3f12a1d95880ad705dbb8035ac763974f57264714856e84d9 EKOHT3.6.6.apk android apk	MoqHao_regex_MultipleDE X MoqHao	[illegible]	451.25 KB	2019-12-23 15:34:26	2019-12-23 17:25:21	1
b8883ab4f78dbe407bee6ba8358bbd9030b2242f927caca5c6928f1b7beaea58 smartcat.apk android 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 android apk	MoqHao_regex_MultipleDE X MoqHao	22 / 62	435.18 KB	2019-12-09 08:21:34	2019-12-23 15:44:59	1
3371118f72444fa2adacaf019c97e0f46d9fbc600117ed0bae99f3e31f9fc4a8 /sagawa4.2.5.apk android 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 android apk	MoqHao_regex_MultipleDE X MoqHao	[illegible]	[illegible]	2019-12-23 03:14:07	2019-12-23 04:16:55	1
6c5550872466bde72d217c6bda8cf77372f0de256a8bdc4ceda7c0c5bf906498 /sagawa8.8.9.apk android apk	MoqHao_regex_MultipleDE X MoqHao	13 / 63	447.05 KB	2019-12-23 03:12:30	2019-12-23 04:14:36	1
2267227bc63e3b3660cada35e854f33075de3644adf62ecfae0b896d02a2ca03 yHxnzDyRoEyvN7uMPva420191223-36210-15tg5al android apk	MoqHao_regex_MultipleDE X MoqHao	15 / 64	450.05 KB	2019-12-23 02:21:56	2019-12-23 03:23:10	1
4b365e1ff416250156d65233e0a53ce99bf14b75f448cc2ffe24cc93832893cd /sagawa9.3.8.apk android apk	MoqHao_regex_MultipleDE X MoqHao	[illegible]	[illegible]	2019-12-23 02:08:23	2019-12-23 03:10:44	1
21b238c28eace817e253071281c0859e0eb263b3285e4115af66b5c0b31a8007 android apk	MoqHao_regex_MultipleDE X MoqHao	15 / 64	451.41 KB	2019-12-23 01:16:04	2019-12-23 02:17:00	1
6382c9a99c6e4b8c1314bce6a135cc8e3dd878992f1c5fa94cb7fda7e2e3b342 android apk	MoqHao_regex_MultipleDE X MoqHao	15 / 64	459.28 KB	2019-12-23 01:10:34	2019-12-23 02:11:36	1

Fake Econt Express

Fake Fedex

Fake Sagawa Express

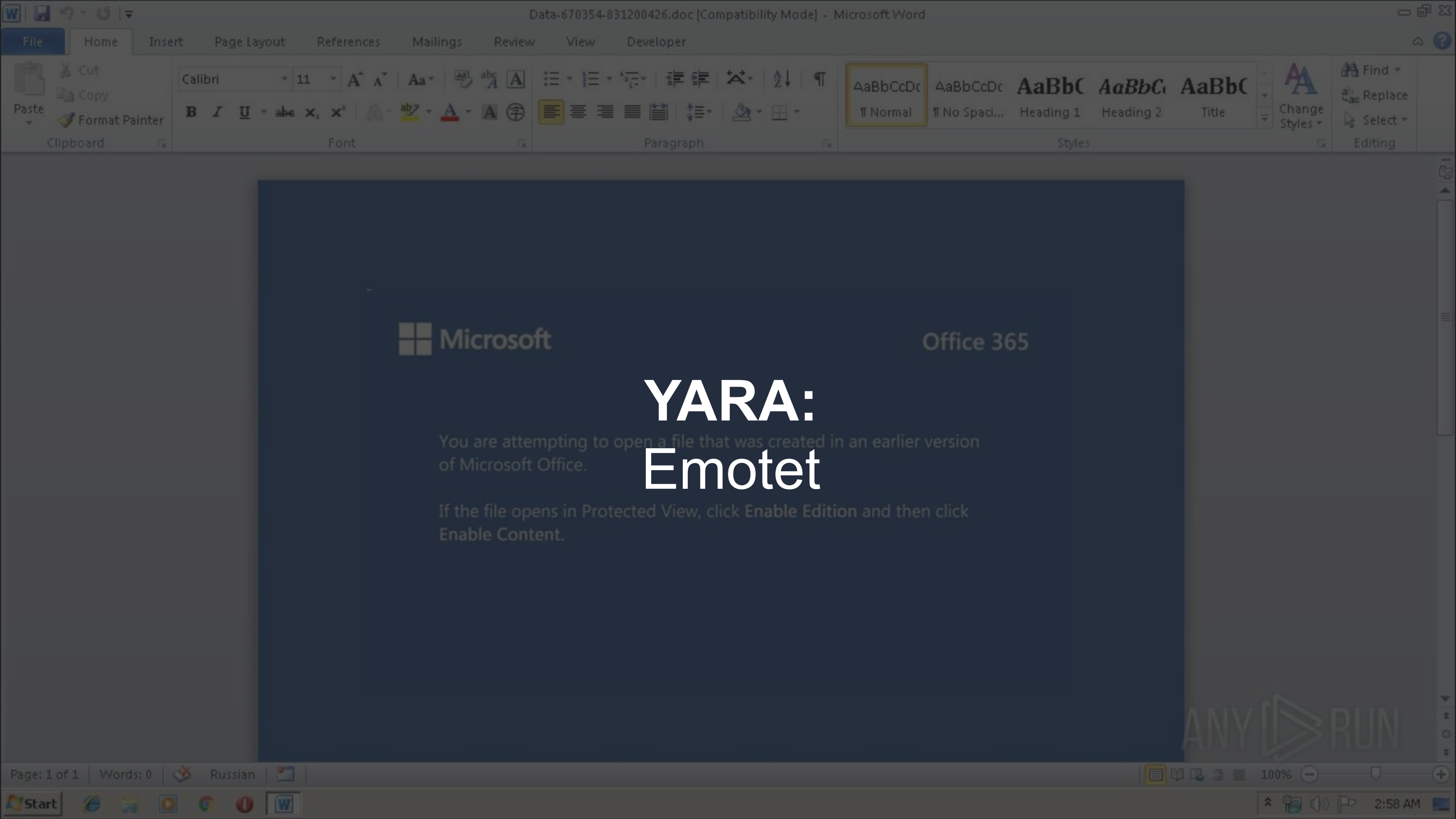
Fake DHL

Fake Sagawa Express

Fake Google Chrome

Fake Sagawa Express

YARA could catch variants of MoqHao. We could know other target brands of MoqHao automatically.



YARA:
Emotet

Data-670354-831200426.doc [Compatibility Mode] - Microsoft Word

Microsoft

Office 365

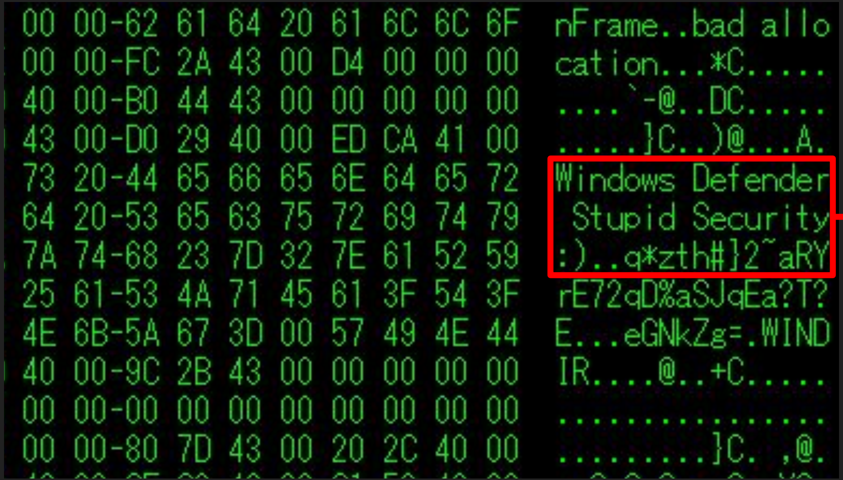
You are attempting to open a file that was created in an earlier version of Microsoft Office.

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

Page: 1 of 1 | Words: 0 | Russian

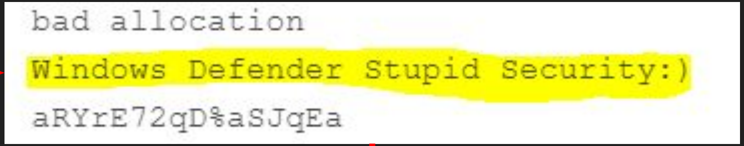
Emotet

- There are ~~ridiculous~~ characteristics strings in the Emotet :).



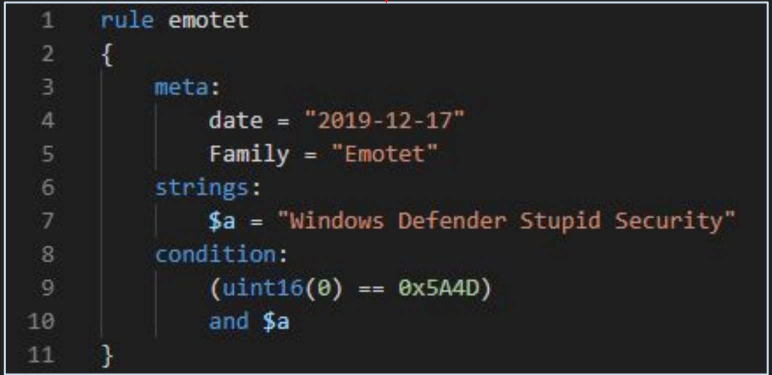
```
00 00-62 61 64 20 61 6C 6C 6F  nFrame..bad allo
00 00-FC 2A 43 00 D4 00 00 00  cation...*C.....
40 00-B0 44 43 00 00 00 00 00  ....`-@..DC.....
43 00-D0 29 40 00 ED CA 41 00  .....]C..)@...A.
73 20-44 65 66 65 6E 64 65 72  Windows Defender
64 20-53 65 63 75 72 69 74 79   Stupid Security
7A 74-68 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
```

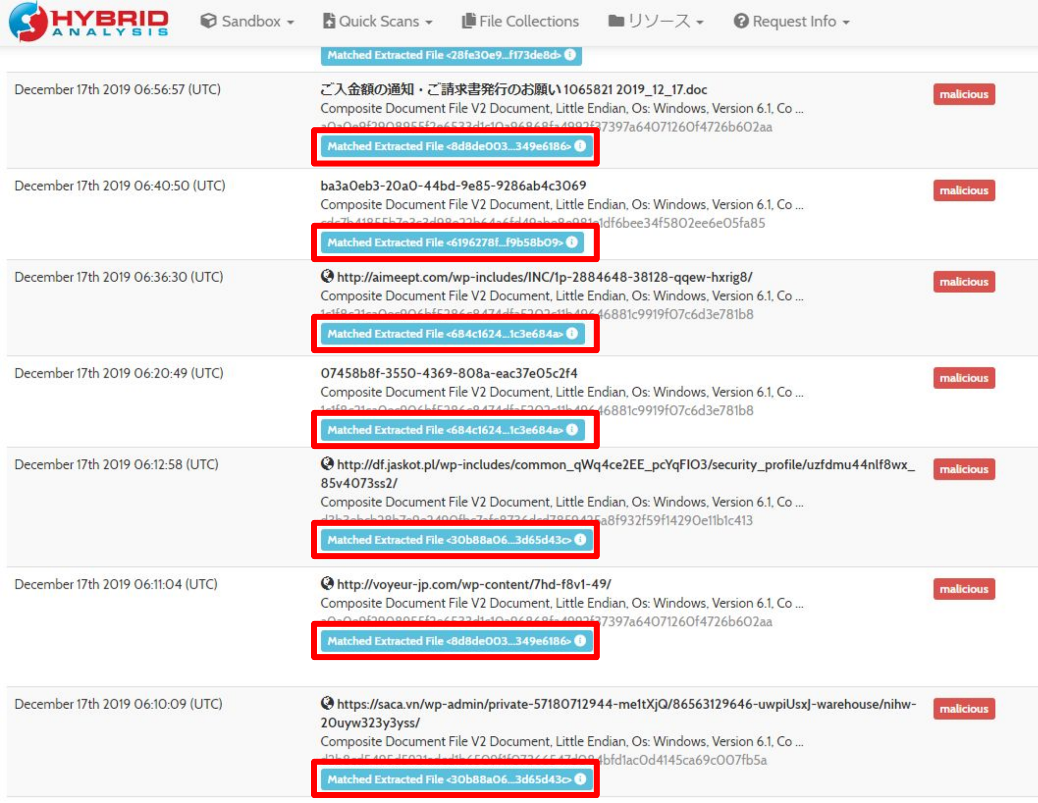
Create a YARA rule by characteristics strings



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

Let's hunt variants of Emotet with this YARA rule!

Search result of Hybrid Analysis with YARA rule for Emotet



Matched Extracted File <28fe30e9...f173de8d>

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 ...
a0a0e9f2908955f2e6533d1c10a96868fa4992f37397a64071260f4726b602aa
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 ...
cdc7b41855b7e3c3d98e22b64a6fd49abe8e981a1df6bee34f5802ee6e05fa85
Matched Extracted File <6196278f...f9b58b09>
malicious

December 17th 2019 06:36:30 (UTC)
http://aimeept.com/wp-includes/INC/1p-2884648-38128-qqew-hxrig8/
Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.1, Co ...
1c1f8c21ca0ec906bf5286c8474dfa5202c11b49646881c9919f07c6d3e781b8
Matched Extracted File <684c1624...1c3e684a>
malicious

December 17th 2019 06:20:49 (UTC)
07458b8f-3550-4369-808a-eac37e05c2f4
Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.1, Co ...
1c1f8c21ca0ec906bf5286c8474dfa5202c11b49646881c9919f07c6d3e781b8
Matched Extracted File <684c1624...1c3e684a>
malicious

December 17th 2019 06:12:58 (UTC)
http://df.jaskot.pl/wp-includes/common_qWq4ce2EE_pcYqFIO3/security_profile/uzfdmu44nlf8wx_85v4073ss2/
Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.1, Co ...
d3b3ebcb28b7e8e2490fbc7afc8736dcd7859425a8f932f59f14290e11b1c413
Matched Extracted File <30b88a06...3d65d43c>
malicious

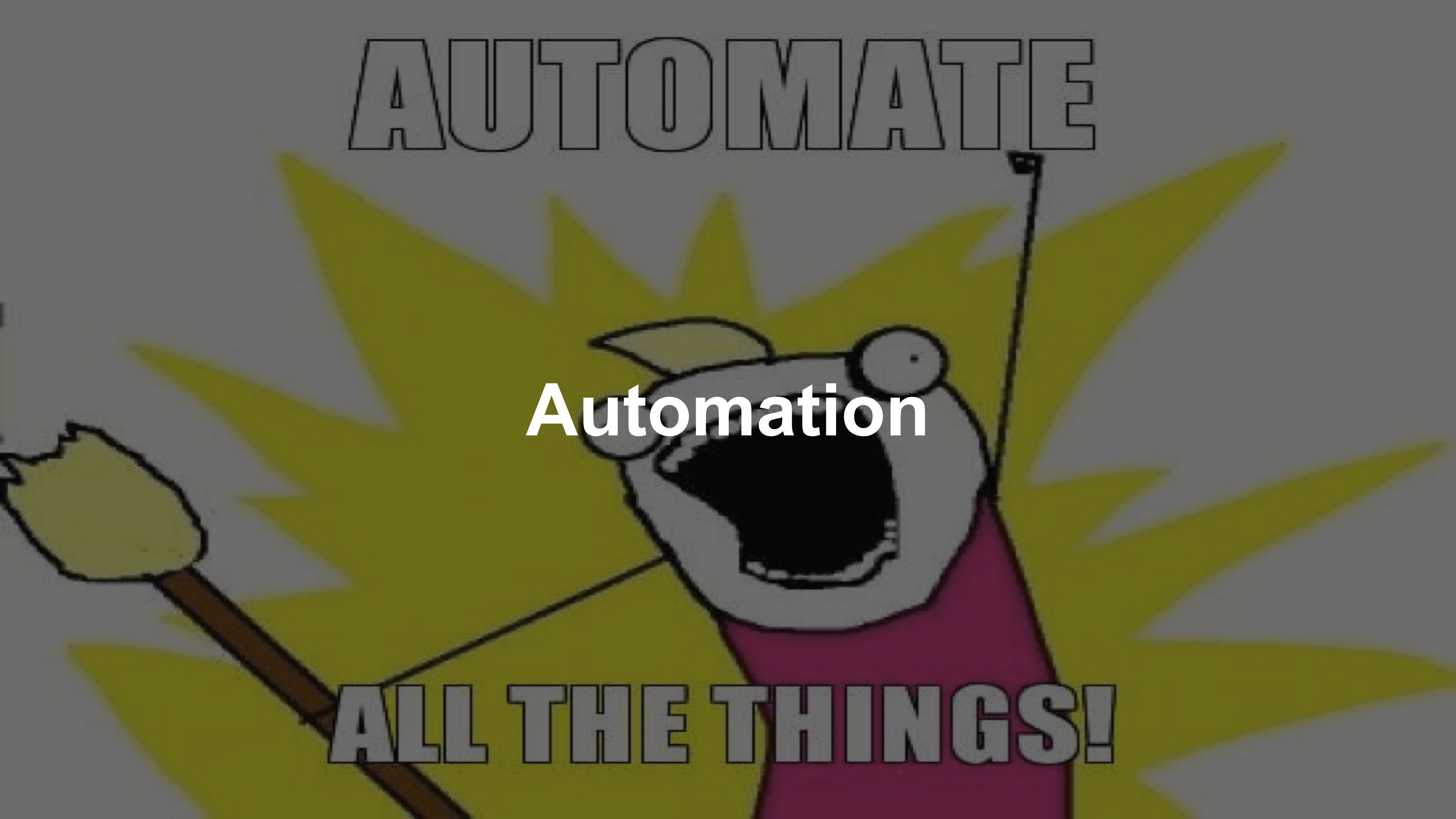
December 17th 2019 06:11:04 (UTC)
http://voyeur-jp.com/wp-content/7hd-f8v1-49/
Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.1, Co ...
a0a0e9f2908955f2e6533d1c10a96868fa4992f37397a64071260f4726b602aa
Matched Extracted File <8d8de003...349e6186>
malicious

December 17th 2019 06:10:09 (UTC)
https://saca.vn/wp-admin/private-57180712944-me1tXjQ/86563129646-uwpiUsxJ-warehouse/nihw-20uyw323y3yss/
Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.1, Co ...
d2b8ad5495d5021cdcd1b6509f1f07366547d984bfd1ac0d4145ca69c007fb5a
Matched Extracted File <30b88a06...3d65d43c>
malicious

Considerations:

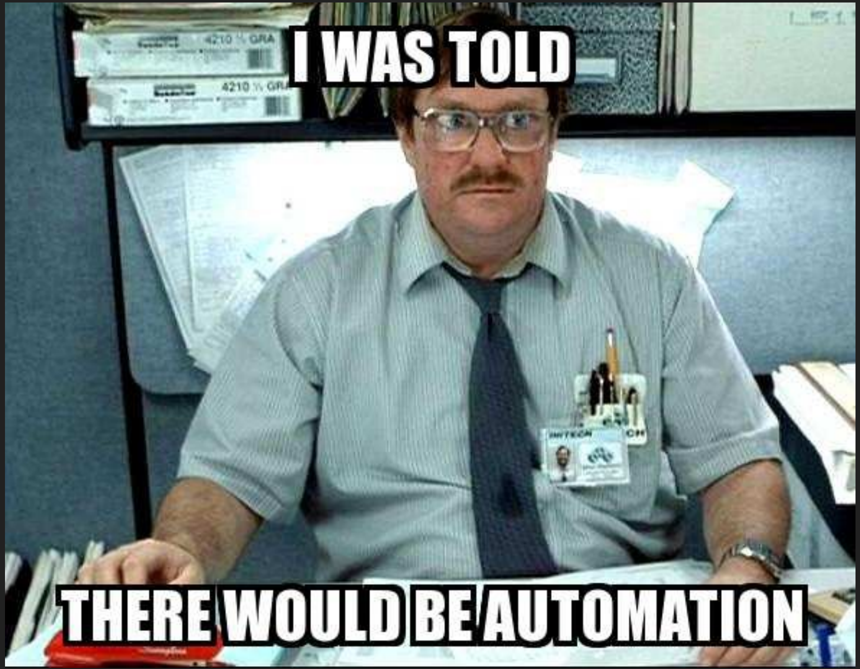
- There are 38 samples in Hybrid Analysis.
- These variants had been used from 16/Dec/2019 to 17/Dec/2019.

Automation



Automation

- Why automation is so important:
  - Automation reduces operating costs.
  - Automation reduces human errors.
  - Making something auto is interesting. 😉

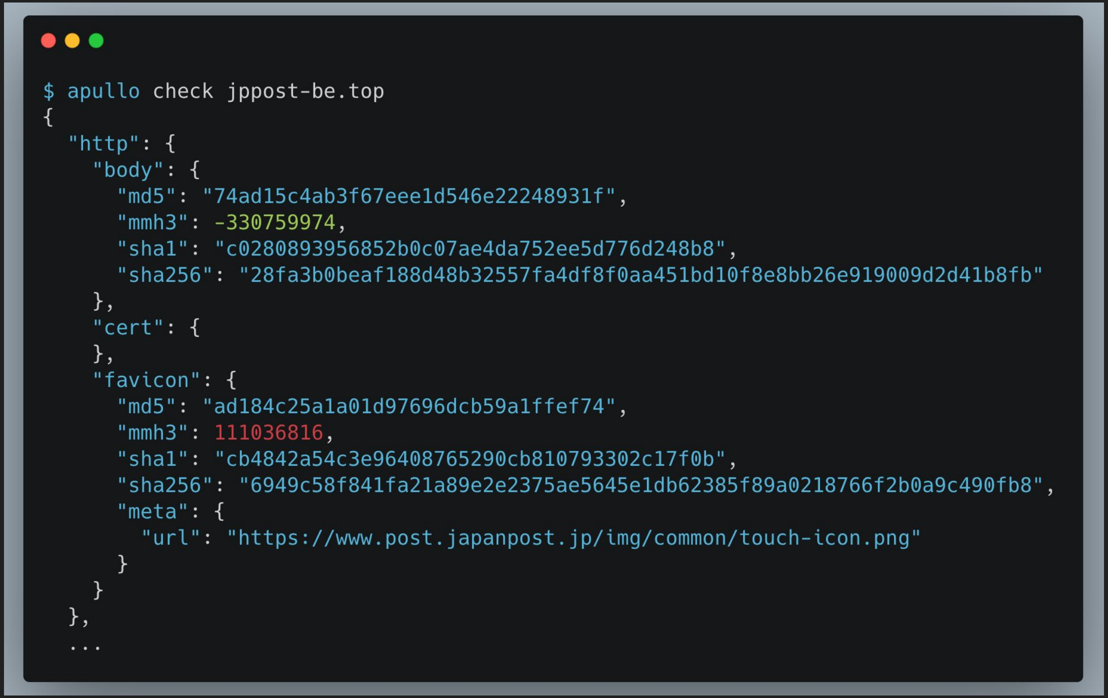


Automation

- Apullo:
  - A tool for taking basic fingerprints of a target.
  - https://github.com/ninoseki/apullo
- Mihari:
  - A monitoring tool leveraging Shodan, Censys, BinaryEdge and etc.
  - https://github.com/ninoseki/mihari
- InQuest/ThreatIngestor:
  - A tool for extract and aggregate threat intelligence.
  - https://github.com/InQuest/ThreatIngestor

Apullo

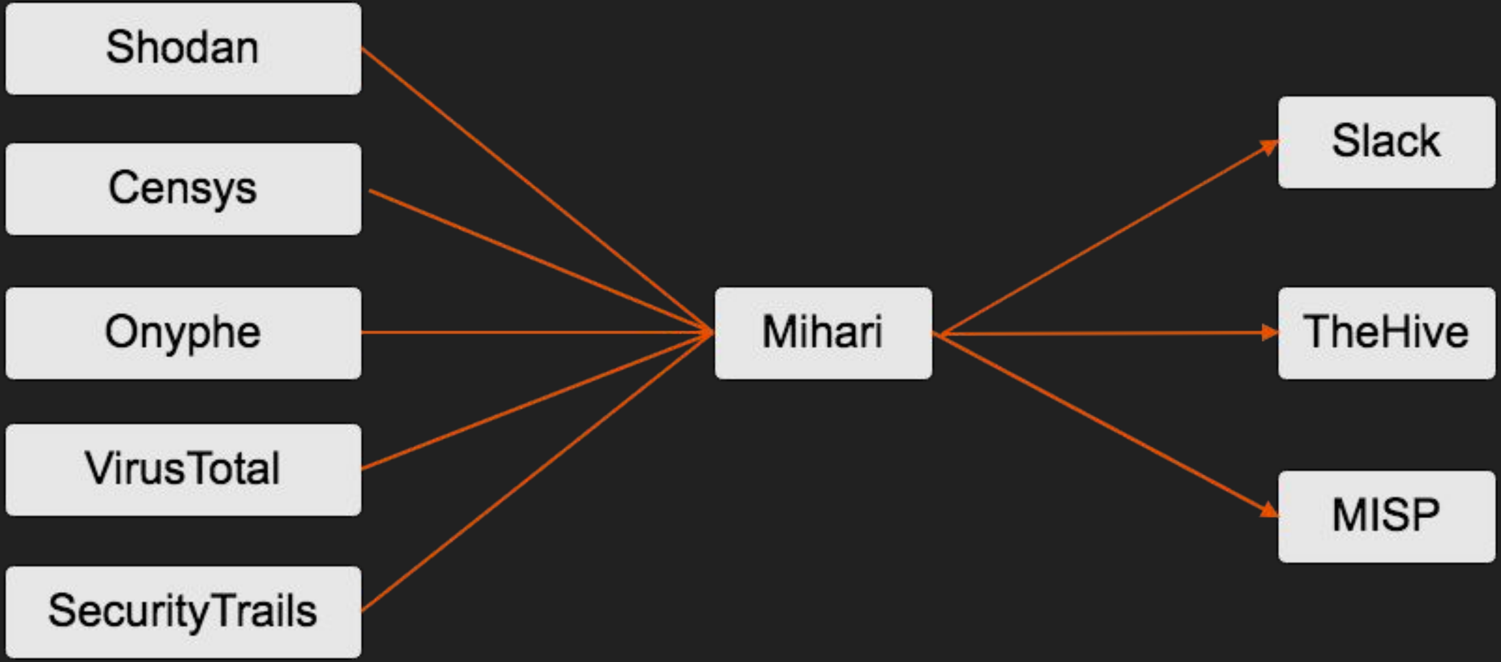
- A tool for taking basic network fingerprints of a target (IP, domain or URL).
  - Hashes of an HTTP response body
  - Hashes of a favicon image
  - Hashes of an SSH host key
  - WHOIS
  - DNS records



```
$ apullo check jppost-be.top
{
  "http": {
    "body": {
      "md5": "74ad15c4ab3f67eee1d546e22248931f",
      "mmh3": -330759974,
      "sha1": "c0280893956852b0c07ae4da752ee5d776d248b8",
      "sha256": "28fa3b0beaf188d48b32557fa4df8f0aa451bd10f8e8bb26e919009d2d41b8fb"
    },
    "cert": {
    },
    "favicon": {
      "md5": "ad184c25a1a01d97696dcb59a1ffef74",
      "mmh3": 111036816,
      "sha1": "cb4842a54c3e964087652 90cb810793302c17f0b",
      "sha256": "6949c58f841fa21a89e2e2375ae5645e1db62385f89a0218766f2b0a9c490fb8",
      "meta": {
        "url": "https://www.post.japanpost.jp/img/common/touch-icon.png"
      }
    }
  },
  ...
```

Mihari

- It’s just a helper to make a query to a search engine and create an alert / event based on results.

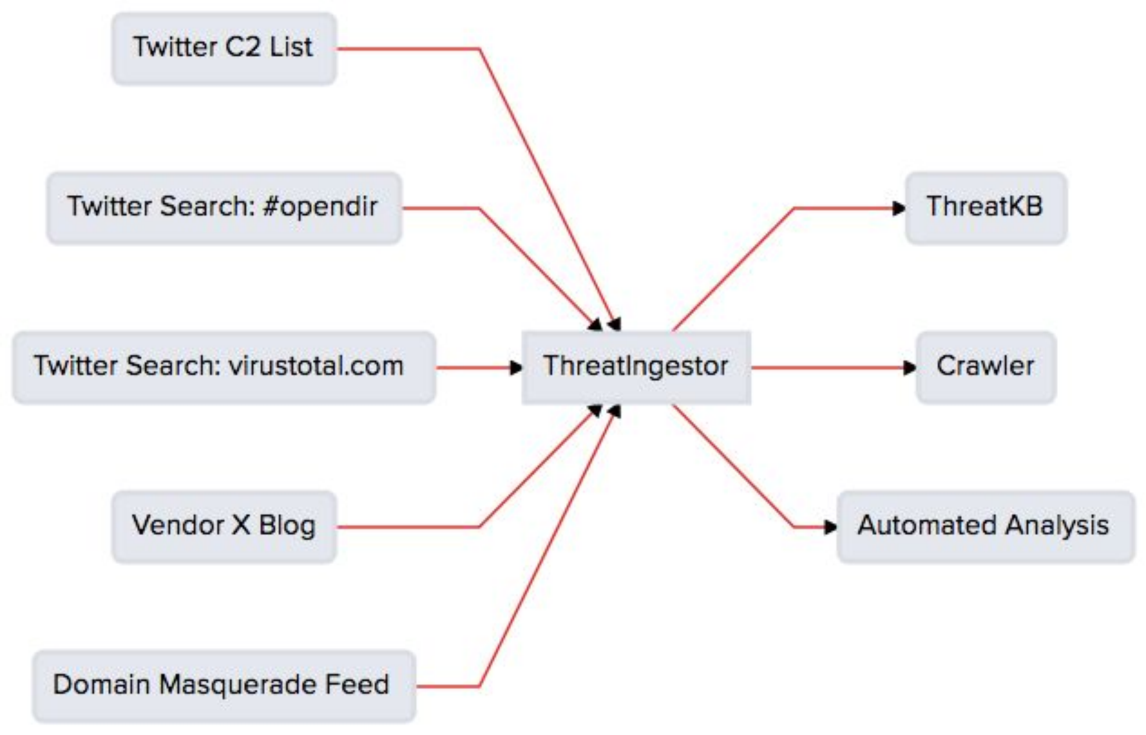


Mihari

- Supported techniques:
  - 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

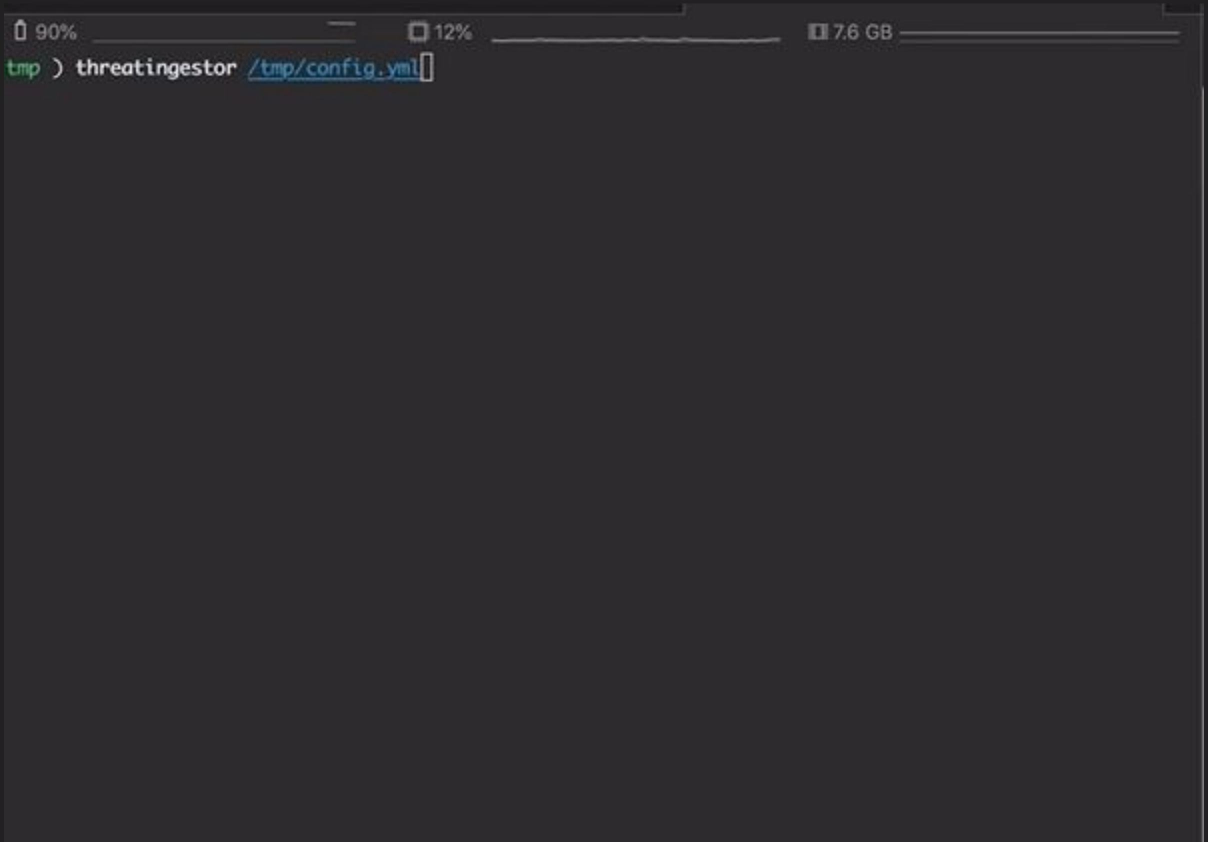
- A deamon behind IOC-DB by InQuest.



ThreatIngestor

- Supported sources:
    - Git repositories, RSS feeds, Generic web pages, etc.
- Supported outputs:
    - CSV files, MISP, MySQL, SQLite, ThreatKB, etc.
- A powerful scraping feature powered by iocextract.
    - https://github.com/InQuest/python-iocextract
- A built-in (dead simple) Web UI.
- Demo

ThreatIngestor



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

Conclusion

Conclusion

- An attacker leaves his fingerprint on site.
    - OSINT makes possible to trace him based on his fingerprint.
- Automation rocks!
    - Automation reduces human errors in investigation.
    - Automation provides a unified way of investigation.
    - Automation reduces operating costs.
- OSINT and automation enable to make an own intelligence for your organization.

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