

MWS 2020

Augma 2020 Dataset

nao_sec

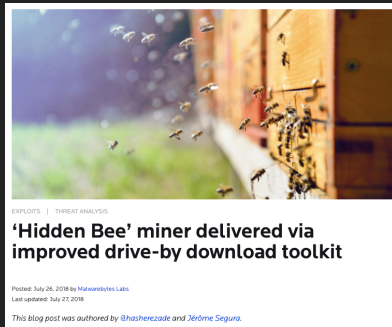
Yosuke Chubachi - Active Defense Institute, LTD.

Rintaro Koike - NTT Security (Japan) KK

Shota Nakajima - Cyber Defense Institute, Inc.

Introduction

DbD Threat Landscape

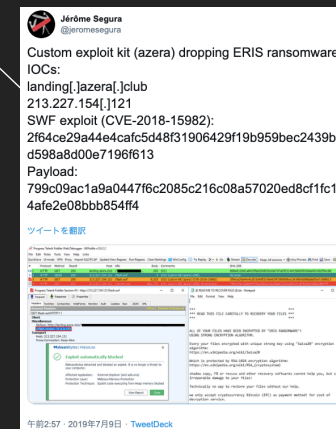


2018-07
Underminer



2019-03
Spelevo

2019-07
azera



2019-08
Lord

**2018-08
Fallout**

Hello "Fallout Exploit Kit"

2018-09-01

First

At the end of August 2018, we observed a new Exploit Kit. Its behavior (code generation using html) and URL pattern are similar to Nuclear Pack Exploit Kit. Therefore we named it "Fallout Exploit Kit". Fallout Exploit Kit is using CVE-2018-4878 and CVE-2018-8174. That code is distinctive and interesting.

**2019-07
Radio**

Weak Drive-by Download attack with "Radio Exploit Kit"

2019-07-15

First

Since July 11 2019, we have observed a new Drive-by Download attack. It is redirected from the ad-network. It does not use a conventional Exploit Kit such as RIG or Fallout, but uses its own exploit kit. We call this "Radio Exploit Kit".

[1] <https://blog.malwarebytes.com/threat-analysis/2018/07/hidden-bee-miner-delivered-via-improved-drive-by-download-toolkit/>

[2] <https://nao-sec.org/2018/09/hello-fallout-exploit-kit.html>

[3] <https://twitter.com/kafeine/status/1103649040800145409>

[4] <https://twitter.com/jeromesegura/status/1148289957716344832>

[5] <https://nao-sec.org/2019/07/weak-dbd-attack-with-radioek.html>

[6] https://twitter.com/adrian_luca/status/1156934215566536705



Our Research

nao_sec
@nao_sec

#RadioEK -> #NEMTY Ransomware
(CC: @malware_traffic, @jeromesegura, @VK_Intel)
app.any.run/tasks/04130377...

ツイートを翻訳

Progress Telerik Fiddler Web Debugger - EKFiddle v.0.9.3.4

#	Result	Protocol	Host	URL	Body	Comments
1	301	HTTP	popcash.net	/world/go/216668/462055	162	
2	200	HTTP	ps.popcash.net	/go/216668/462055	426	
3	303	HTTP	ps.popcash.net	/ad/ad?p=216668&w=462055&t=38c08b4...	48	
4	200	HTTP	45.147.198.206	/	3,542	Radio EK (HTML/JS) (Landing Page)
5	200	HTTPS	iplogger.com	/11kvc	116	Network fingerprinting (URI)
6	200	HTTPS	iplogger.com	/11kvc	116	Network fingerprinting (URI)
7	200	HTTP	45.147.198.206	/supra.exe	231,936	
8	200	HTTP	api.lipify.org	/	14	
9	200	HTTP	api.db-ip.com	/v2/free/153.249.74.119/countryName	5	
10	200	HTTPS	dist.torproject.org	/torbrowser/8.5.5/tor-win32-0.4.1.5.zip	0	

nao_sec
@nao_sec

#FalloutEK -> #Raccoon Stealer (v1.2)
app.any.run/tasks/51f9adaf...

ツイートを翻訳

Progress Telerik Fiddler Web Debugger - EKFiddle v.0.9.3.4

#	Result	Protocol	Host	URL	Body	Comments
1	200	HTTP	www.1q2w3e5tyb.com	/	731	
2	200	HTTPS	adexchange4u.com	/S1n5/bkx2/JpVJD	5,169	Fallout EK (Landing Page)
3	200	HTTPS	adexchange4u.com	/MGK/27_07_19807Lb=Visoring_tedesch...	29,012	Fallout EK (JS Code)
4	200	HTTPS	adexchange4u.com	/Fq7/1994-06-11/liquidise	7,596	Fallout EK (Encoded Data 1)
5	200	HTTPS	adexchange4u.com	/1986-10-17/w1w?eJer=JyZm8lenora=690...	28,652	Fallout EK (Encoded Data 2)
6	200	HTTPS	adexchange4u.com	/8635_Crouch/MWMRLK	35,139	Fallout EK (CVE-2018-15982)
7	200	HTTPS	adexchange4u.com	/Mw/Ew/piddlers?EVgCK=byrewoman_cy...	5,805	Fallout EK (Encoded PowerShell)

nao_sec
@nao_sec

#PseudoGate -> #GrandSoftEK -> #Ramnit
app.any.run/tasks/d3226768...

Progress Telerik Fiddler Web Debugger - EKFiddle v.0.9.3.2

#	Result	Protocol	Host	URL	Body	Comments
1	200	HTTP	kohikan.space	/	11,058 (01)	PseudoGate
2	200	HTTP	bfmbn.terminating.promodscounter-tokyo.host	/anyways_respondingfrog	530 (02)	GrandSoft EK (HTML/JS) (Landing Page)
3	200	HTTP	bfmbn.terminating.promodscounter-tokyo.host	/getversional/1/2/3/4	21,185 (03)	GrandSoft EK (URI) (Landing Page)
4	200	HTTP	bfmbn.terminating.promodscounter-tokyo.host	/1/9/3/4	316,184 (04)	GrandSoft EK (URI) (Payload)

nao_sec
@nao_sec

#RigEK -> #SmokeLoader -> #Danabot + #SystemBC +
#Vidar (v13.1) + #Quasar RAT + #CrySis Ransomware
+ #Predator + #SmokeLoader
app.any.run/tasks/086e4aa9...

Progress Telerik Fiddler Web Debugger - EKFiddle v.0.9.3.4

#	Result	Protocol	Host	URL	Body	Comments
1	302	HTTPS	btcseller.club	/	0 (01)	
2	302	HTTP	at2tds17.world	/fn84fhweuf	0 (02)	Redirection to RIG EK (Headers)
3	200	HTTP	188.225.26.246	/?MTMjNjgw&PKRTOCVK8BArdq=known...	144,870 (03)	RIG EK (URI) (Landing Page)
4	200	HTTP	188.225.26.246	/?OTM2NTM=&dSRwgT&CGKzocLQxW=be...	6,570 (04)	RIG EK (URI) (Flash Exploit)
5	200	HTTP	188.225.26.246	/?MY3C31&QX7/BC1bATW&AcCrHq2	758,048 (05)	RIG EK (URI) (Payload)



Motivation of Development "Augma"

- **A drive-by threat is still "ACTIVE"**
 - Many attack campaigns and EKs have appeared
- **Manual drive-by observation is too hard**
- **We want to research the latest threat trends automatically**
 - Active Observation + Analysis + Extraction



Challenges of Exploit Kit Crawling

- **Anti-Cloaking**

- EK and malware distribution infrastructure BAN specific IP address and range
- Example, TrendMicro, Symantec and public cloud IP range is BANNED by RIG EK

- **Behaving:**

- Evading checks of Ad-networks

- **Chasing:**

- Crawling target selection is difficult

- **Accuracy:**

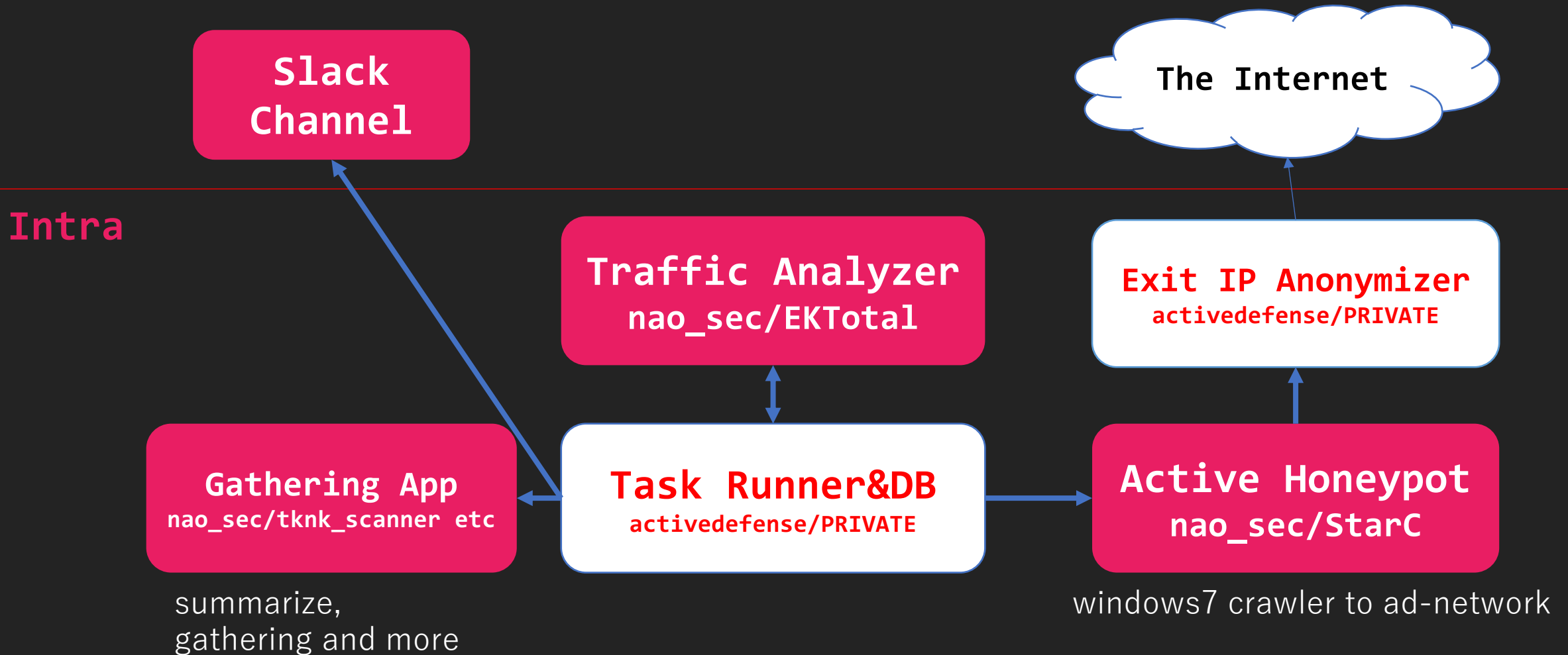
- Need reliable detection rules

Augma :

An automated active observation platform



Augma Overview





Active Honeygot (StarC)

- **Simple high-interactive client honeypot**
 - <https://github.com/nao-sec/starc>
 - Input a URL, StarC access and collect data
 - Traffic data (pcap & saz)
 - Screenshot
 - Temp directory files



Traffic Analyzer (EKTOTAL)

- Automatic DbD traffic analyzer
 - <https://github.com/nao-sec/ektotal>
- Input a pcap or saz, EKTOTAL analyze traffic data
 - Identify campaign & EK
 - Extract some information
 - Encode key
 - CVE Number
 - SWF file
 - Malware
 - Detecting with EKfiddle's rules and Augma custom rules
 - <https://github.com/malwareinfosec/EKfiddle>
 - Lazy "Gate Estimation" added on July, 2019



Lazy “Gate Estimation”

- Gate

- We call “Gate” that campaign specific redirect server
- EKTotal can estimate Gate
- This function helps identify and categorize campaigns
- Some campaigns NOT go through Gate

```
[Alert] Estimated Gate
[URL] http[:]//searchenginenaavigation.com/

[Alert] RIG EK (Landing Page)
[URL] http[:]//176.57.215.119/?
MzYyMDA3&JHLcz&eMctiz=detonator&OUqauMkc=perpetual&TfJnRTq=referred&HTJ
Mv3DSKNbnkjWHViPxomG9MildZmqZGX_k7TDff-qoVvcCgWR&TwUJWklw=strategy&GOYY
eeBRawTp3E3WKgwzz4YIUlMVo66tj0iBwRLO05_Q_UePMAJNrKKlJLL_mhj2&JUA1Av=det

[Alert] RIG EK (SWF Payload)
[URL] http[:]//176.57.215.119/?
MTgyMzc2&NYQnAuGPvb&xBxIGSuDmVC=vest&evLWuAZa=everyone&gcFxInLWVEz=crit
xomG9MildZaqZGX_k7vDff-qoVxcCgWRxfp&khFQFndqkZV=known&HezjBi=already&qX
eeBRawrp3E3WKgwzz4YIUlWVo66tj0mBwRLO05DQ_UePMANNrKKTE7k83m2ZiLZCQA&aqGH
artfelt&GvIuzYskCuGIyWL=referred&pdJGLt=difference&yYOIBKxsJDsHMzkyODM1
```



Finally...

#dbd 9月20日 (金)

CTD_Bot アプリ 18:47

[Alert] Redirection to RIG EK (Estimated Gate)
[URL] http[:]//www.playbucket.com/

[Alert] RIG EK (Landing Page)
[URL] http[:]//2.59.41.10/?
MTA3NTAw&DPZJFu&HgyYJcGz=vest&KoZJBf=community&ffhd3s=w3bQMvXcJxjQFYbGMv3DSKNbNkjWHVipXoaG9MildZmqZX_k7rDFF-qoVrcCgWR&qsFjJp=heartfelt&usATqk=difference&GQScKWHgI=golfer&LEOVsm=constitution&t4gdgfg4=xFuRKLZUPQvjjkHWKQ0z1YpeB1Ib96CnjkmDmkSVg56AqReFNQ0R9qK1JLZ_mhj2&sJJsoZKu=referred&JhzgGIZD=everyone&teEVLd=blackmail&wzzCTDq=heartfelt&eOLqam=everyone&ggTf0tJO=wrapped&yFvr=known&np1W=criticized&tszc=strategy&jjQcVtpaw0TMzMDc=

18:47 [Alert] RIG EK (SWF Payload)
[URL] http[:]//2.59.41.10/?MzA4MjE0&OPHxcBQFwmQ&QhESVuBornCRvC=known&t4gdgfg4=mYhZVl0T9a6tikaDmx0DiZ-G_h3YaQNF9pWcFLhti1WnxrkXcsJzxRCKvWkExeItUFwV4QwTm6f7Vam0-0da&QaWtmRckj=detonator&UcPMmVraSrP=everyone&jJseImUtDVwLI=heartfelt&vgLwls&nc&K&QJfWl&ziZSeo=blackmail&Y=dlx=vest&HsqxAUpvoR=known&enxAPgZFhWzE=detonator&HSnrxU0=perpetual&EfKaWKTo&vzoz&hor&rv&AZXX&communi&sbahMjoF=constitu&tion&ozt0FSviiuynehh=perpetual&ffhd3s=xHbQMrbYbRnFFYrfKPLEUK1EMUnWA0GKw&Zhan&mx&_G&15&VWdCFu&D&HI&1ULAS&n&HTA0qhgGE=known&SrtVuKqNTA2Mjkz

CTD_Bot アプリ 21:12

[Alert] Estimated Gate
[URL] http[:]//makemoneyzywith.me/?utm_id=10893&utm_campaign=Worldwidepop&utm_source=367435635&utm_cost=0.001

[Alert] Fallout EK (Landing Page)
[URL] https[:]//assdrill.biz/6325/recaution_foreguess_Birses.aspx

[Alert] Fallout EK
[URL] https[:]//assdrill.biz/cankorous/Verity/beclap?stallboat=Whipship

[Alert] FalloutEK (Landing Page)
[URL] https[:]//assdrill.biz/Trustor/Weedling_4743_Cloudlets/prelegal/Urorrhea.aspx

RIG EK

#dbd 9月10日 (木)

CTD_Bot アプリ 17:22

[Alert] Estimated Gate
[URL] https[:]//shorico.club/404.php

[Alert] Underminer EK
[URL] https[:]//shorico.xyz/index.php?
ad_id=V2RUXoUTaVRd8kUJH9AT9g&re=V2RUXoUTaVRd8kUJH9AT9g&rt=V2RUXoUTaVRd8kUJH9AT9g&id=9088&zone=V2RUXoUTaVRd8kUJH9AT9g&prod=V2RUXoUTaVRd8kUJH9AT9g&lp=Type&st=V2RUXoUTaVRd8kUJH9AT9g&e=1568881335&y=203389073274

[Alert] Underminer EK
[URL] https[:]//shorico.xyz/js/3o259dkamu4s0m9rgm612luf5s.js

CTD_Bot アプリ 18:22

[Alert] Estimated Gate
[URL] https[:]//shorico.club/404.php

[Alert] Underminer EK
[URL] https[:]//shorico.xyz/index.php?
ad_id=sRdykDzrGIF129pWrRm32A&re=sRdykDzrGIF129pWrRm32A&rt=sRdykDzrGIF129pWrRm32A&id=9088&zone=sRdykDzrGIF129pWrRm32A&prod=sRdykDzrGIF129pWrRm32A&lp=Type&st=sRdykDzrGIF129pWrRm32A&e=1568884938&y=203389076877

18:22 [Alert] Underminer EK
[URL] https[:]//shorico.xyz/js/e67ia8b07g9jhsqk2gfbpqddno.js

CTD_Bot アプリ 18:32

[Alert] Estimated Gate
[URL] http[:]//digalitol.fun/trawa.php

[Alert] Fallout EK (Landing Page)
[URL] https[:]//yourglassinass.com/pacing_Ta&time=01&b2?Q/8432

[Alert] Fallout EK
[URL] https[:]//yourglassinass.com/Bhangi-Pivotable/11377.html

Underminer EK

FALLOUT EK

Augma 2020 Dataset Overview



Augma 2020 Dataset

- **Period:** 2019/05-2020/04
- **Data:**
 - Captured malicious traffic as Fiddler saz format and pcapng format.
- **Files and Directories:**
 - `augma2020/augma2020dataset.description.en.txt`
 - `augma2020/augma2020dataset.description.ja.txt`
 - `augma2020/ek/ek.metadata.tsv`
 - `augma2020/ek/samples/{*.pcap and * .saz}`
 - `augma2020/tss/tss.metadata.tsv`
 - `augma2020/tss/samples/{*.pcap and * .saz}`
 - `augma2020/unidentifiedek/samples/`



Statistics

(Unit: file)

All threats potentially target to Japan
(Augma uses JP related IP Addresses)

pcap: 10020

- ek: 7418
- tss: 2544
- unidentifiedek: 58

saz: 10008

- ek: 7419
- tss: 2544
- unidentifiedek: 45



Our Dataset Covered almost EKs in the wild

	Underminer EK	Fallout EK	GrandSoft EK	RIG EK	Spelevo EK	Capesand EK	Radio EK	Lord EK	Bottle EK	Custom EK(azera)	KaiXin	月次総計
Total	5176	583	520	443	103	59	35	19	9	4	1	6952
May-19	449	0	17	72	0	0	0	0	0	0	1	539
Jun-19	682	30	13	49	8	0	0	0	0	0	0	782
Jul-19	456	11	10	10	0	0	0	0	0	4	0	491
Aug-19	0	3	57	101	86	0	0	19	0	0	0	266
Sep-19	16	189	39	42	0	0	35	0	0	0	0	321
Oct-19	263	182	40	9	9	0	0	0	0	0	0	503
Nov-19	601	25	94	2	0	17	0	0	0	0	0	739
Dec-19	812	32	121	27	0	42	0	0	0	0	0	1034
Jan-20	1040	20	118	27	0	0	0	0	0	0	0	1205
Feb-20	255	51	11	32	0	0	0	0	5	0	0	354
Mar-20	510	39	0	72	0	0	0	0	4	0	0	625
Apr-20	92	1	0	0	0	0	0	0	0	0	0	93



Example (metadata)

TSV(Tab Separated Values):
1 line per 1 crawl

```
date:2019/05/01 00:10:02
saz:ek/samples/2019-05-01_00-10-02.saz
pcap:ek/samples/2019-05-01_00-10-02.pcap
name:Underminer EK
mal_url:http://27.122.57.192:9081/index.php?ad_id={snipped}
name:Underminer EK
mal_url:http://27.122.57.192:9081/js/bhfsbqqpvs9nr61tnqqou0lr8g.js
```

- Identifier derives from EKfiddle's rule and Augma custom rule
- Some rules define another identifier on same EK detection like GrandSoft(Checker) and GrandSoft(Landing)



Attention

- You **SHOULD** refer to published article[7] when you publish anything with this dataset
- You **MUST** pay attention to use IP, URL and payloads in this dataset. It is potentially malicious

[7] Rintaro Koike and Yosuke Chubachi, "Finding drive-by rookies using an automated active observation platform", VirusBulletin 2019, Oct. 2019.

Any Questions?



Twitter: @nao_sec

Email: info@nao-sec.org