Finding drive-by rookies using an automated active observation platform

Rintaro Koike (NTT Security Japan KK)

Yosuke Chubachi (Active Defense Institute, LTD)

Who are we?

- **Rintaro Koike**
  - SOC Analyst & Threat Researcher @ NTT Security Japan
  - Founder & Researcher @ nao_sec
- **Yosuke Chubachi**
  - One-man Start-up CEO/Founder @ Active Defense Institute, Ltd.
  - Active Defense provides:
    - Tactical Cyber Threat Intelligence Service focused on DbD
    - Consulting, Pentest and Hands-on Training
  - Researcher and operator of this automation system @ nao_sec
- **nao_sec**
  - Security Research Team (NOT COMPANY)
  - Independent & Non-Profit

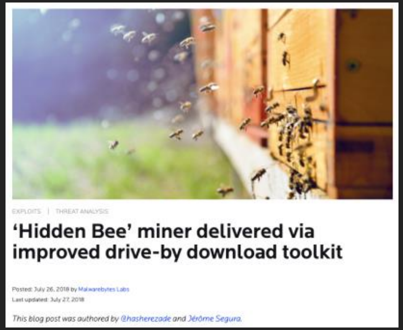
Copyright©2019 nao_sec All Rights Reserved.

Introduction

Copyright©2019 nao_sec All Rights Reserved.

DbD Threat Landscape

2018-07
Underminer



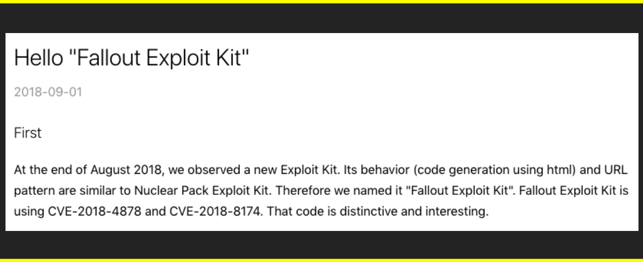
EXPLOITS | THREAT ANALYSIS

‘Hidden Bee’ miner delivered via improved drive-by download toolkit

Posted: July 26, 2018 by Malwarebytes Labs
Last updated: July 27, 2018

This blog post was authored by @hasherezade and Jérôme Segura.

2018-08
Fallout



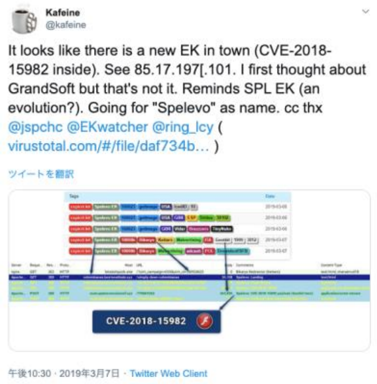
Hello "Fallout Exploit Kit"

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.

2019-03
Spelevo



Kafeine
@kafeine

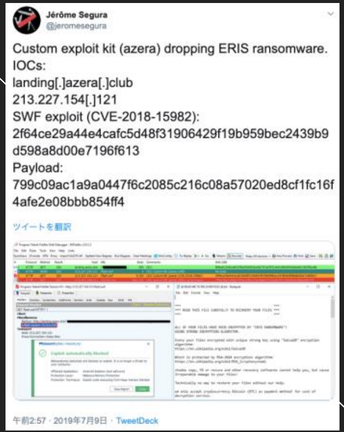
It looks like there is a new EK in town (CVE-2018-15982 inside). See 85.17.197[.101. I first thought about GrandSoft but that's not it. Reminds SPL EK (an evolution?). Going for "Spelevo" as name. cc thx @jspchc @EKwatcher @ring_lcy (virustotal.com/#/file/daf734b…)

ツイートを翻訳

CVE-2018-15982

午後10:30 · 2019年3月7日 · Twitter Web Client

2019-07
azera



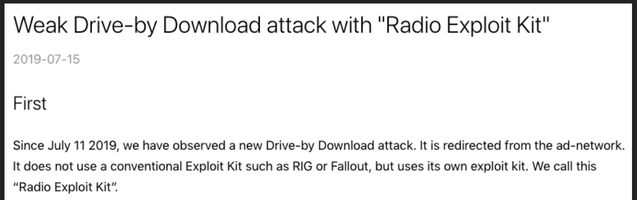
Jérôme Segura
@jeromesegura

Custom exploit kit (azera) dropping ERIS ransomware.
IOCs:
landing[.]azera[.]club
213.227.154[.]121
SWF exploit (CVE-2018-15982):
2f64ce29a44e4cafc5d48f31906429f19b959bec2439b9d598a8d00e7196f613
Payload:
799c09ac1a9a0447f6c2085c216c08a57020ed8cf1fc16f4afe2e08bbb854ff4

ツイートを翻訳

午前2:57 · 2019年7月9日 · TweetDeck

2019-07
Radio



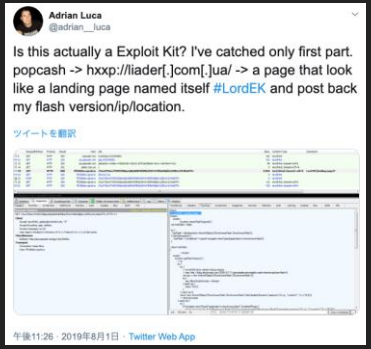
Weak Drive-by Download attack with "Radio Exploit Kit"

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”.

2019-08
Lord



Adrian Luca
@adrian__luca

Is this actually a Exploit Kit? I've catched only first part. popcash -> hxxp://liader[.]com[.]ua/ -> a page that look like a landing page named itself #LordEK and post back my flash version/ip/location.

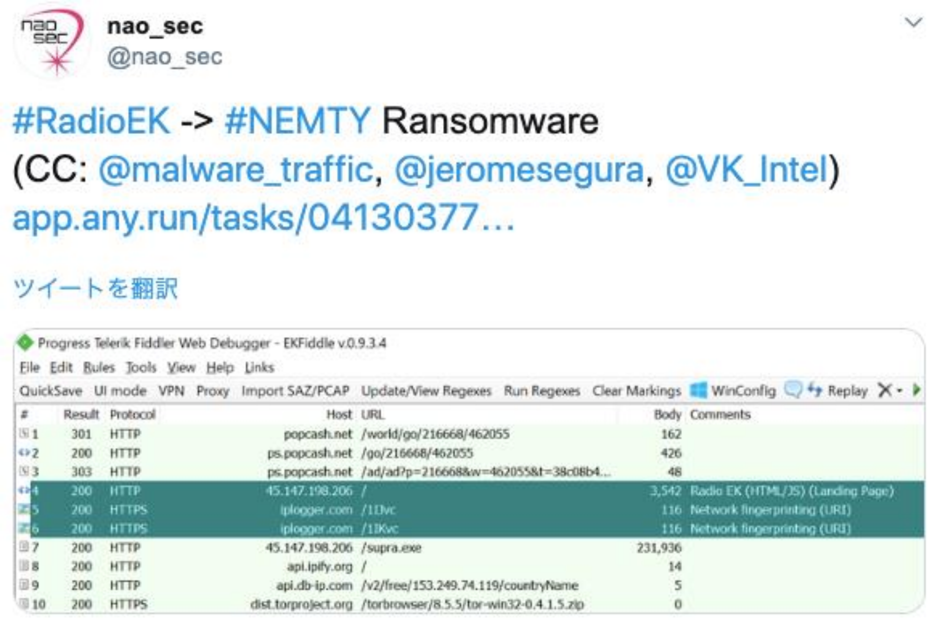
ツイートを翻訳

午後11:26 · 2019年8月1日 · Twitter Web App

[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

Copyright©2019 nao_sec All Rights Reserved.

Our Research



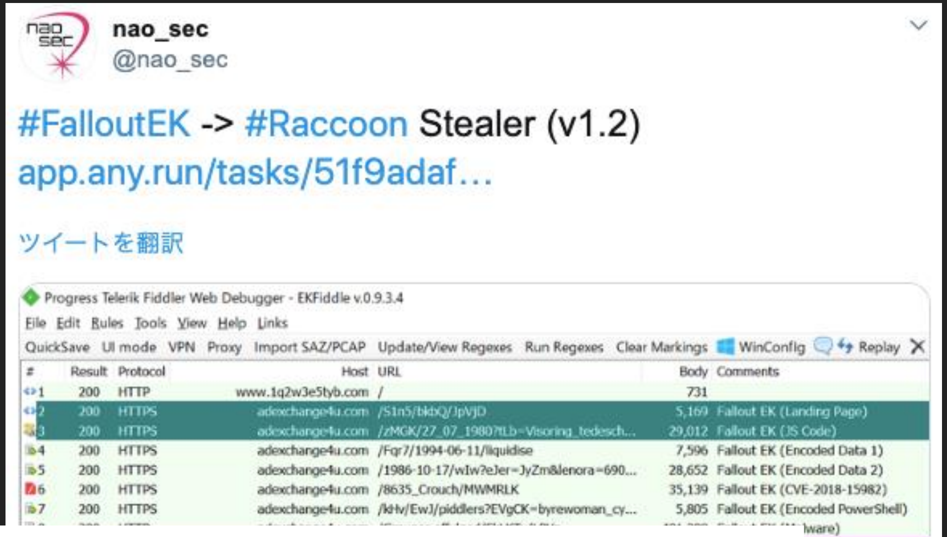
nao_sec
@nao_sec

#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	/1IJvc	116	Network fingerprinting (URI)
6	200	HTTPS	iplogger.com	/1IKvc	116	Network fingerprinting (URI)
7	200	HTTP	45.147.198.206	/supra.exe	231,936	
8	200	HTTP	api.ipify.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	



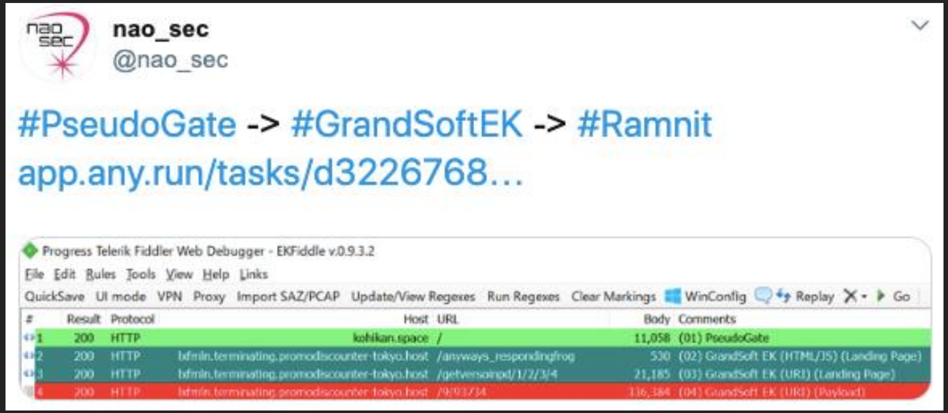
nao_sec
@nao_sec

#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/bkbQ/JpVjD	5,169	Fallout EK (Landing Page)
3	200	HTTPS	adexchange4u.com	/zMGK/27_07_1980?tLb=Visoring_tedesch...	29,012	Fallout EK (JS Code)
4	200	HTTPS	adexchange4u.com	/Fqr7/1994-06-11/liquidise	7,596	Fallout EK (Encoded Data 1)
5	200	HTTPS	adexchange4u.com	/1986-10-17/wIw?eJer=JyZm&lenora=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	/kHv/EwJ/piddlers?EVgCK=byrewoman_cy...	5,805	Fallout EK (Encoded PowerShell)
						ware)
						C2 (URI)
						C2 (URI)

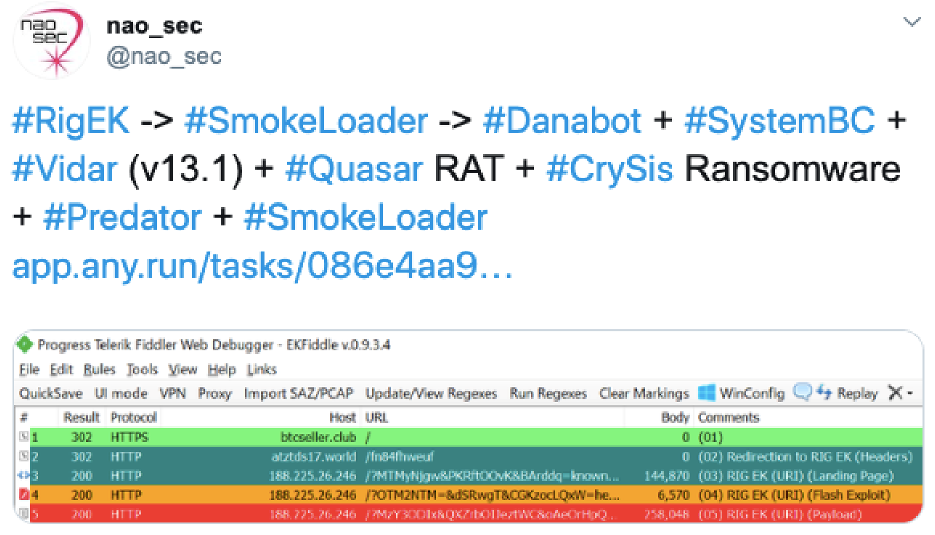


nao_sec
@nao_sec

#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	bfmln.terminating.promodiscounter-tokyo.host	/anyways_respondingfrog	530	(02) GrandSoft EK (HTML/JS) (Landing Page)
3	200	HTTP	bfmln.terminating.promodiscounter-tokyo.host	/getversoinpd/1/2/3/4	21,185	(03) GrandSoft EK (URI) (Landing Page)
4	200	HTTP	bfmln.terminating.promodiscounter-tokyo.host	/9/93734	136,384	(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	atztds17.world	/fn84fhweuf	0	(02) Redirection to RIG EK (Headers)
3	200	HTTP	188.225.26.246	/?MTMyNjgw&PKRftOOvK&BArddq=known...	144,870	(03) RIG EK (URI) (Landing Page)
4	200	HTTP	188.225.26.246	/?OTM2NTM=&dSRwgT&CGKzocLQxW=he...	6,570	(04) RIG EK (URI) (Flash Exploit)
5	200	HTTP	188.225.26.246	/?MzY3ODIx&QXZrbOIJezIWC&oAeOrHpQ...	258,048	(05) RIG EK (URI) (Payload)

Copyright©2019 nao_sec All Rights Reserved.

Motivation

- Drive-by Download attack is still “ACTIVE”
  - Many attack campaigns and EKs have appeared

- Very difficult to observe manually
- Too late since the incident occurred

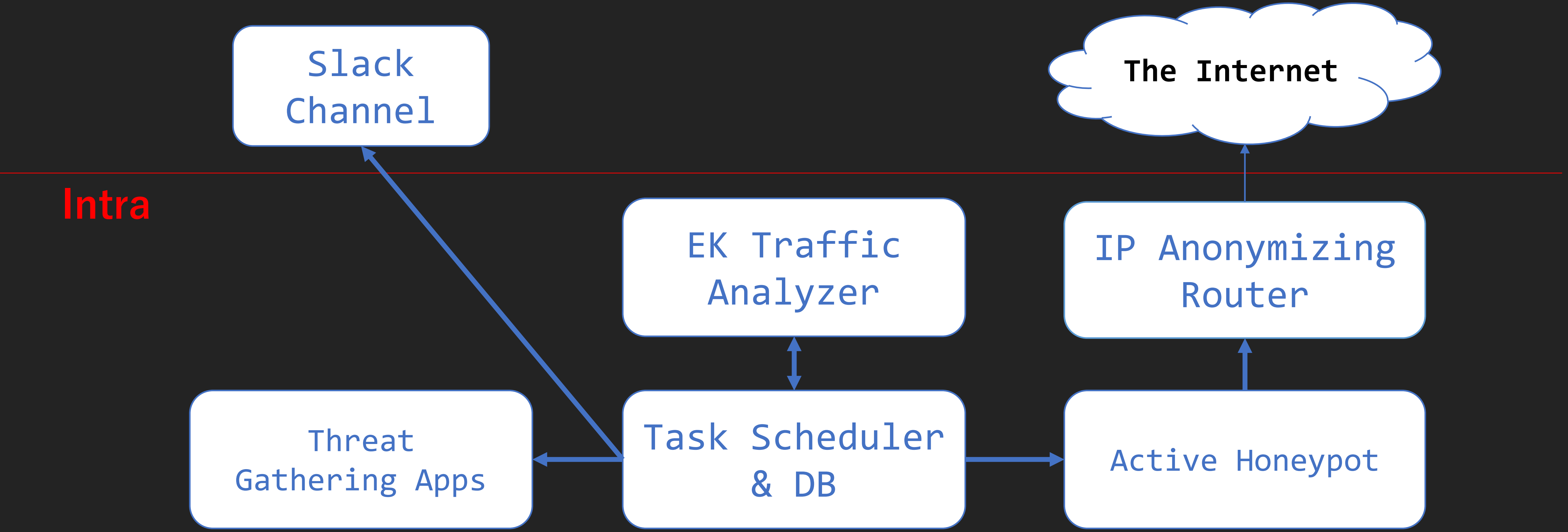
- Want to research the latest threat trends automatically
  - Active Observation + Analysis + Extraction

Copyright©2019 nao_sec All Rights Reserved.

An automated active observation platform

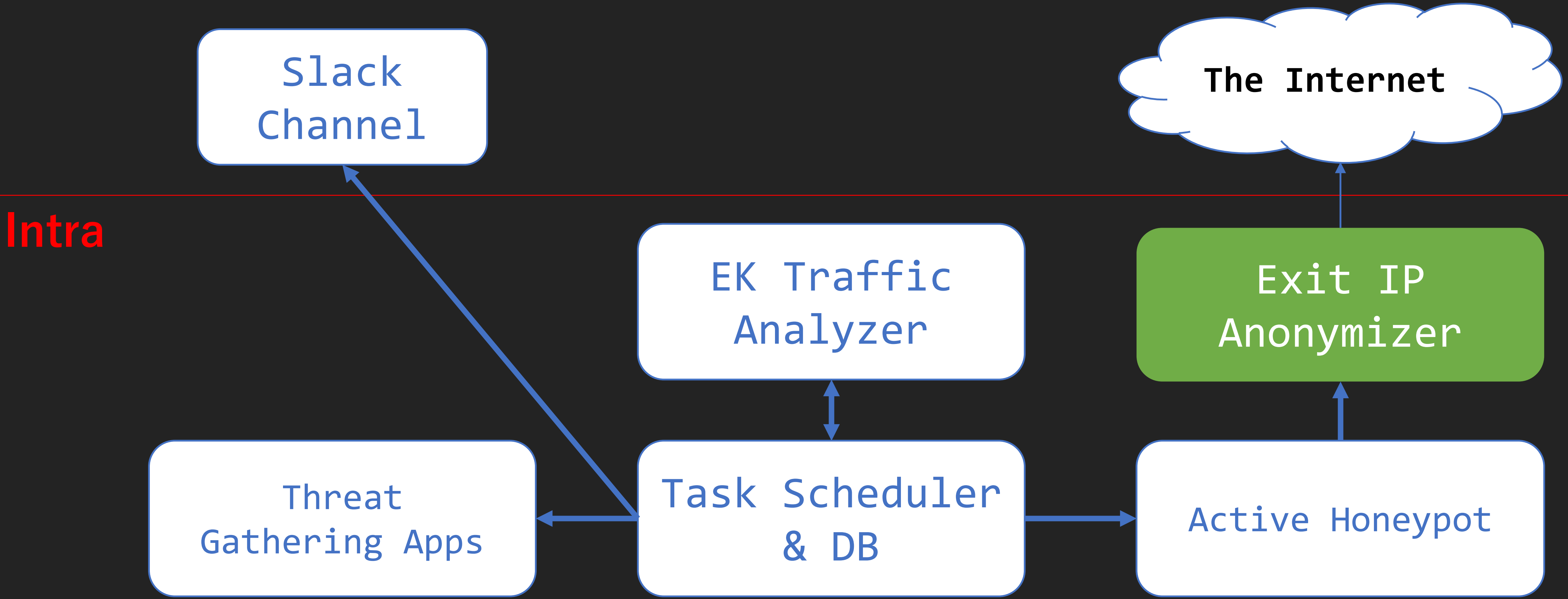
Copyright©2019 nao_sec All Rights Reserved.

Our Observation Platform Overview



Copyright©2019 nao_sec All Rights Reserved.

First, Exit IP Anonymizer



Copyright©2019 nao_sec All Rights Reserved.

Problems of Exploit Kit Crawling

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

- **Also ad-network BANNED web-crawler because…**
    - Crawling access is malicious activity to ad-network lol

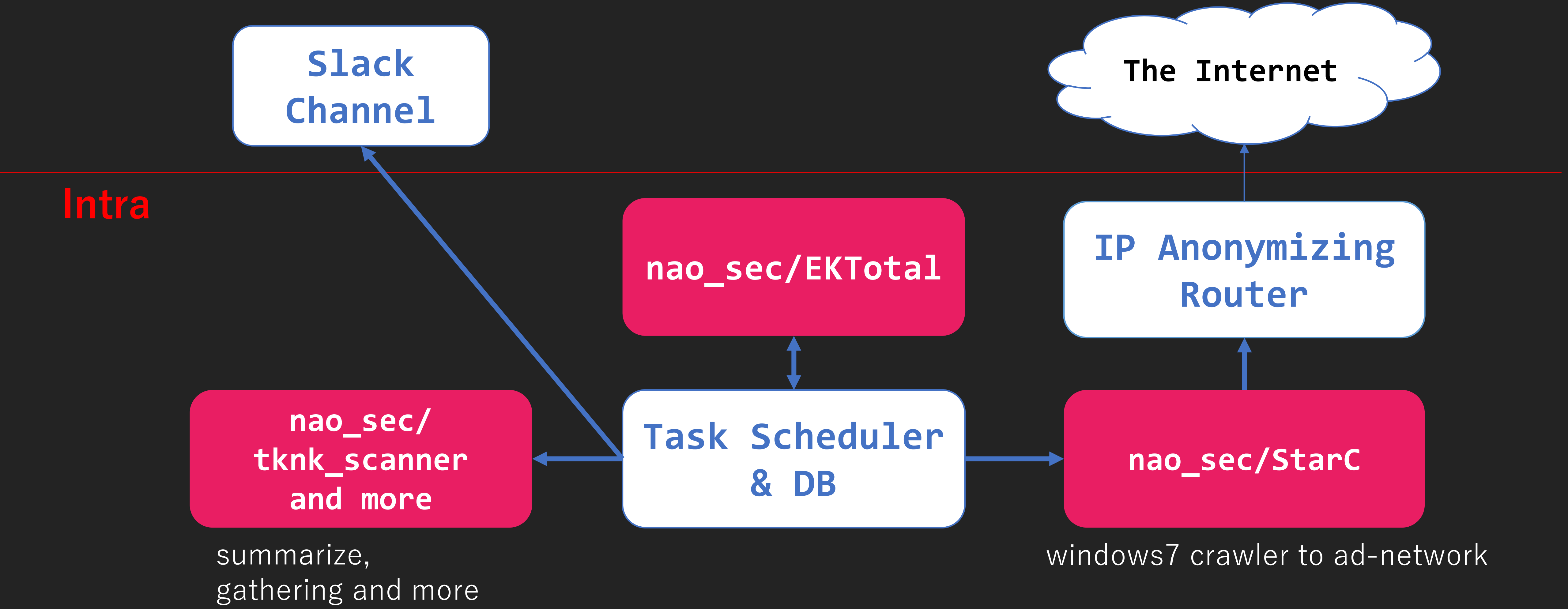
Copyright©2019 nao_sec All Rights Reserved.

Need Exit IP Addresses more and more!

- Popular Solution: VPN Services
- Better Solution: VPNGate(more variety IPs)
- Our Solution:

Copyright©2019 nao_sec All Rights Reserved.

Next: nao_sec OSS Tools overview



summarize, gathering and more

windows7 crawler to ad-network

Copyright©2019 nao_sec All Rights Reserved.

Active Honeypot (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

Copyright©2019 nao_sec All Rights Reserved.

EK Traffic Analyzer (EKTotal)

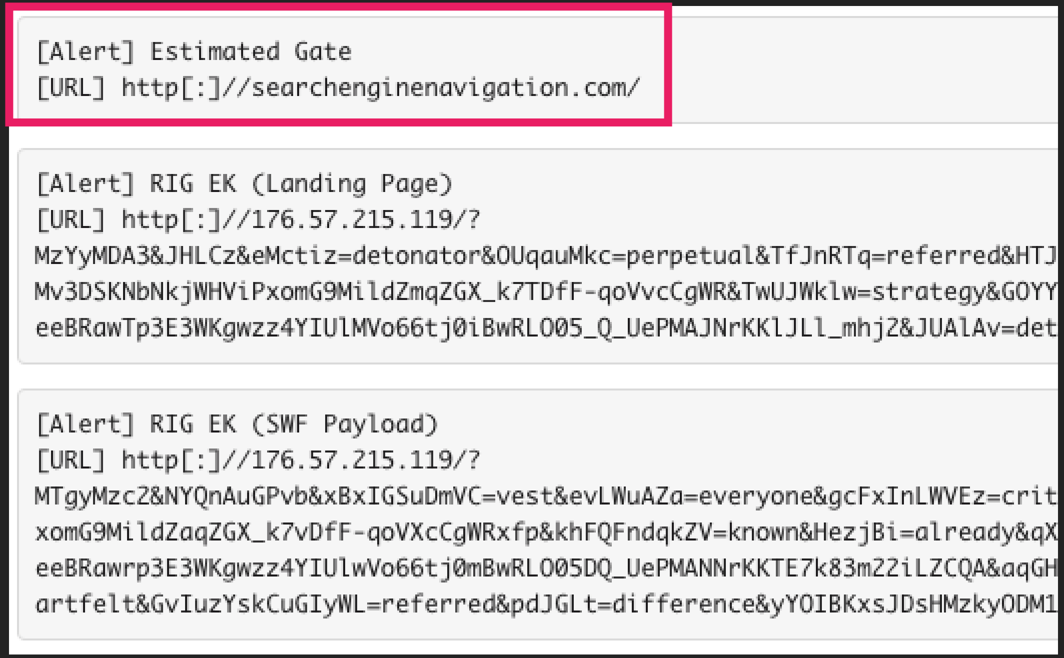
- **Automatic DbD traffic analyzer**
  - https://github.com/nao-sec/ektotal

  - Input a pcap or saz, EKTotal analyze traffic data
    - Identify campaign & EK
    - Extract some information
      - Encode key
      - CVE Number
      - SWF file
      - Malware
    - Depends on EKFiddle’s rules
      - https://github.com/malwareinfosec/EKFiddle
    - Lazy “Gate Estimation” added on July, 2019

Copyright©2019 nao_sec All Rights Reserved.

Lazy “Gate Estimation”

- Gate
  - Always leads to EK if you meet certain conditions
  - EKTotal can estimate Gate
  - This function helps identify and categorize campaigns



```
[Alert] Estimated Gate
[URL] http[:]//searchenginenavigation.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_mhjZ&JUAlAv=det

[Alert] RIG EK (SWF Payload)
[URL] http[:]//176.57.215.119/?
MTgyMzcZ&NYQnAuGPvb&xBxIGSuDmVC=vest&evLWuAZa=everyone&gcFxInLWVEz=crit
xomG9MildZaqZGX_k7vDfF-qoVXcCgWRxfp&khFQFndqkZV=known&HezjBi=already&qX
eeBRawrp3E3WKgwzz4YIUlwVo66tj0mBwRLO05DQ_UePMANNrKKTE7k83mZ2iLZCQA&aqGH
artfelt&GvIuzYskCuGIyWL=referred&pdJGLt=difference&yYOIBKxsJDsHMzkyODM1
```

Copyright©2019 nao_sec All Rights Reserved.

Malware Identifier (tknk_scanner)

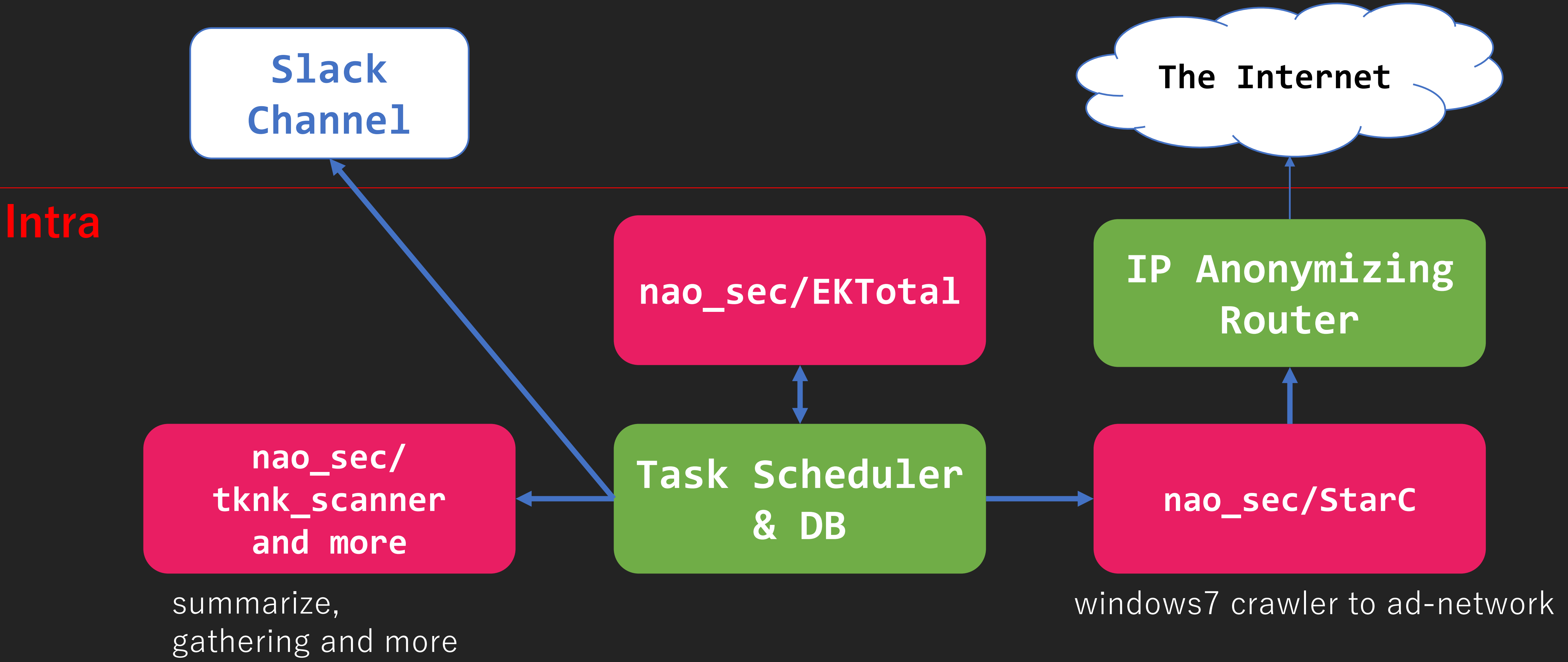
- tknk_scanner developed by Shota Nakajima and Keita Nomura @nao_sec
  - This tool introduced at Black Hat Europe 2018 Arsenal

- Fast Malware Identifier
  - Throw extracted unidentified binary by EKTotal

- https://github.com/nao-sec/tknk_scanner

Copyright©2019 nao_sec All Rights Reserved.

Workflow: Complex API calling :-<

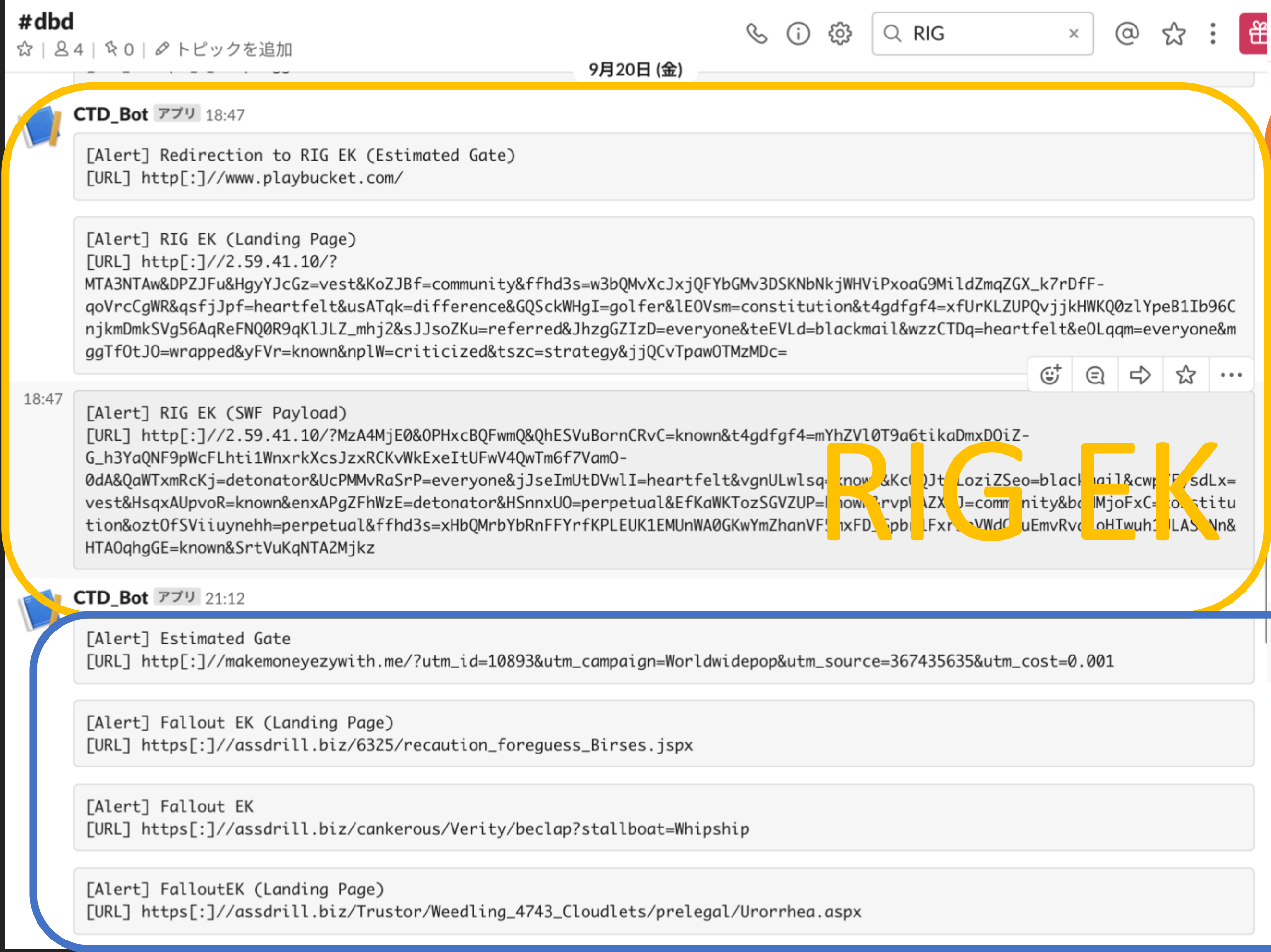


summarize,
gathering and more

windows7 crawler to ad-network

Copyright©2019 nao_sec All Rights Reserved.

Finally...



RIG EK

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=w3bQMvXcJxjQFYbGMv3DSKNbNkjWHViPxoaG9MildZmqZGX_k7rDfF-
qoVrcCgWR&qsfjJpf=heartfelt&usATqk=difference&GQSckWHgI=golfer&lEOVsm=constitution&t4gdfgf4=xfUrKLZUPQvjjkHWKQ0zlYpeB1Ib96C
njkmDmkSVg56AqReFNQ0R9qKlJLZ_mhj2&sJJsoZKu=referred&JhzgGZIzD=everyone&teEVLd=blackmail&wzzCTDq=heartfelt&eOLqqm=everyone&m
ggTf0tJO=wrapped&yFVr=known&nplW=criticized&tszc=strategy&jjQCvTpaw0TMzMDc=
```

18:47

```
[Alert] RIG EK (SWF Payload)
[URL] http[:]//2.59.41.10/?MzA4MjE0&OPHxcBQFwmQ&QhESVuBornCRvC=known&t4gdfgf4=mYhZVl0T9a6tikaDmxDOiZ-
G_h3YaQNF9pWcFLhti1WnxrkXcsJzxRCKvWkExeItUFwV4QwTm6f7VamO-
0dA&QaWTxmRcKj=detonator&UcPMMvRaSrP=everyone&jJseImUtDVwlI=heartfelt&vgnULwlsq=known&KcQJt[illegible]LoziZSeo=blackmail&cwp[illegible]sdLx=
vest&HsqxAUpvoR=known&enxAPgZFhWzE=detonator&HSnnxUO=perpetual&EfKaWKTozSGVZUP=known&rvpl[illegible]AZX[illegible]J=community&bc[illegible]MjoFxC=constitu
tion&oztOfSViiuynehh=perpetual&ffhd3s=xHbQMrbYbRnFFYrfKPLEUK1EMUnWA0GKwYmZhanVF5[illegible]xFD_Spb[illegible]lFxr[illegible]VWdQ[illegible]uEmvRv[illegible]oHTwuh1[illegible]LAS[illegible]Nn&
HTAOqhgGE=known&SrtVuKqNTA2Mjkz
```

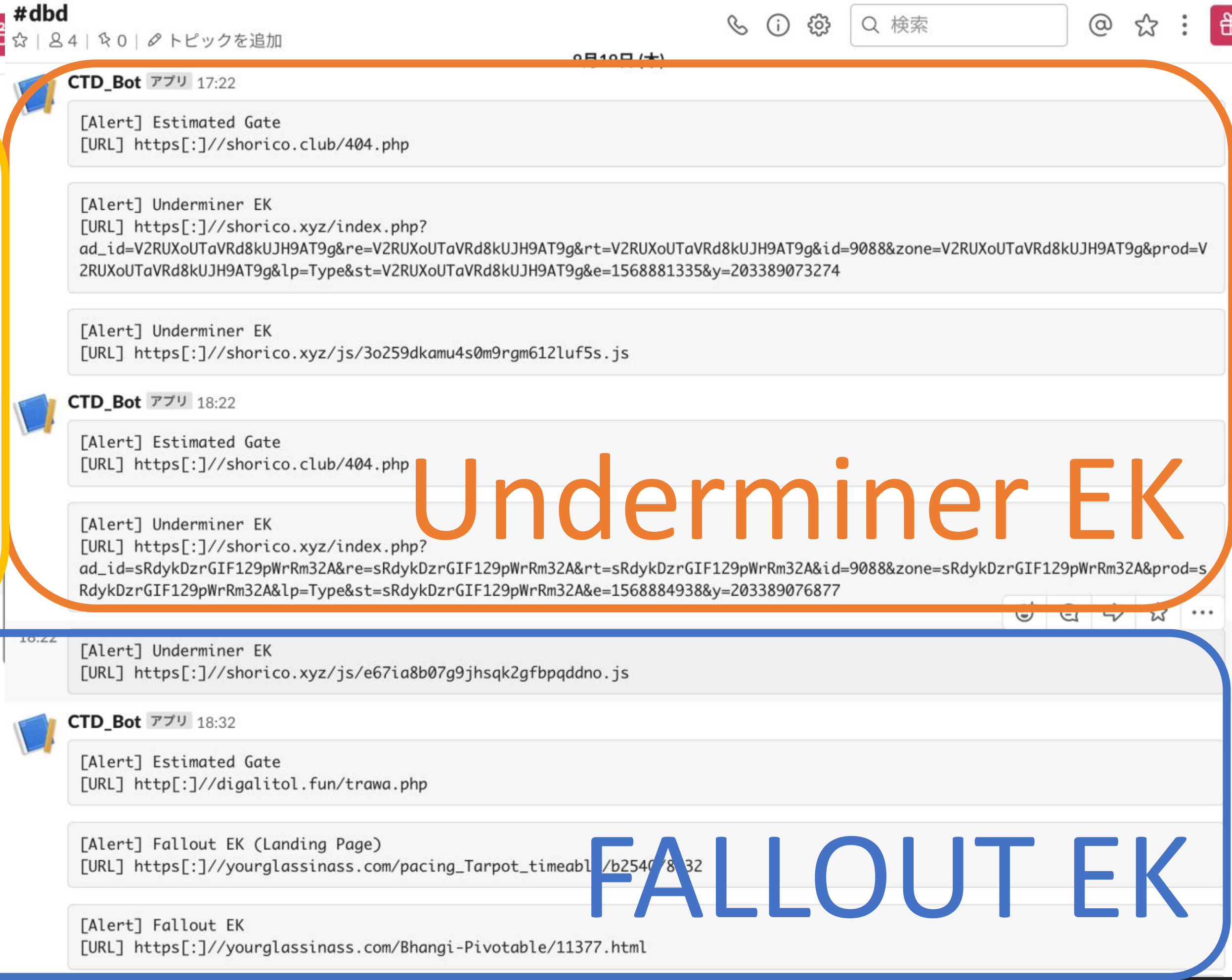
CTD_Bot アプリ 21:12

```
[Alert] Estimated Gate
[URL] http[:]//makemoneyezywith.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.jspx
```

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

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



Underminer EK

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=V
2RUXoUTaVRd8kUJH9AT9g&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=s
RdykDzrGIF129pWrRm32A&lp=Type&st=sRdykDzrGIF129pWrRm32A&e=1568884938&y=203389076877
```

18:22

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

FALLOUT EK

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_Tarpot_timeabl[illegible]/b254[illegible]8[illegible]32
```

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

Copyright©2019 nao_sec All Rights Reserved.

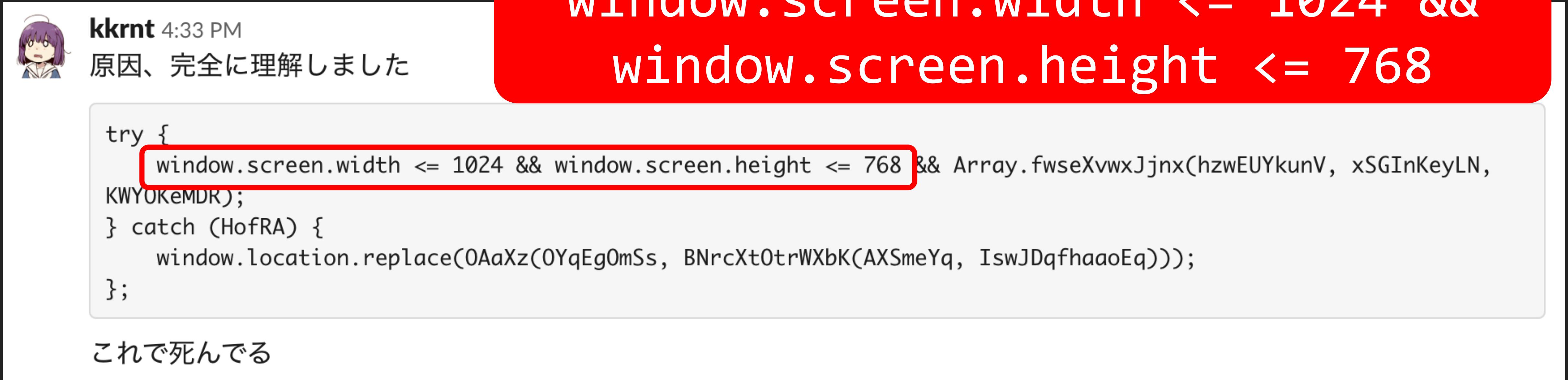
Try & Error

- Defeating Anti-Sandbox
- Selection Seed of Crawling
- Persistence of Crawling

Copyright©2019 nao_sec All Rights Reserved.

Defeating Anti-Sandbox:
Sandbox Detection by Display Resolution

window.screen.width <= 1024 &&
window.screen.height <= 768



kkrnt 4:33 PM

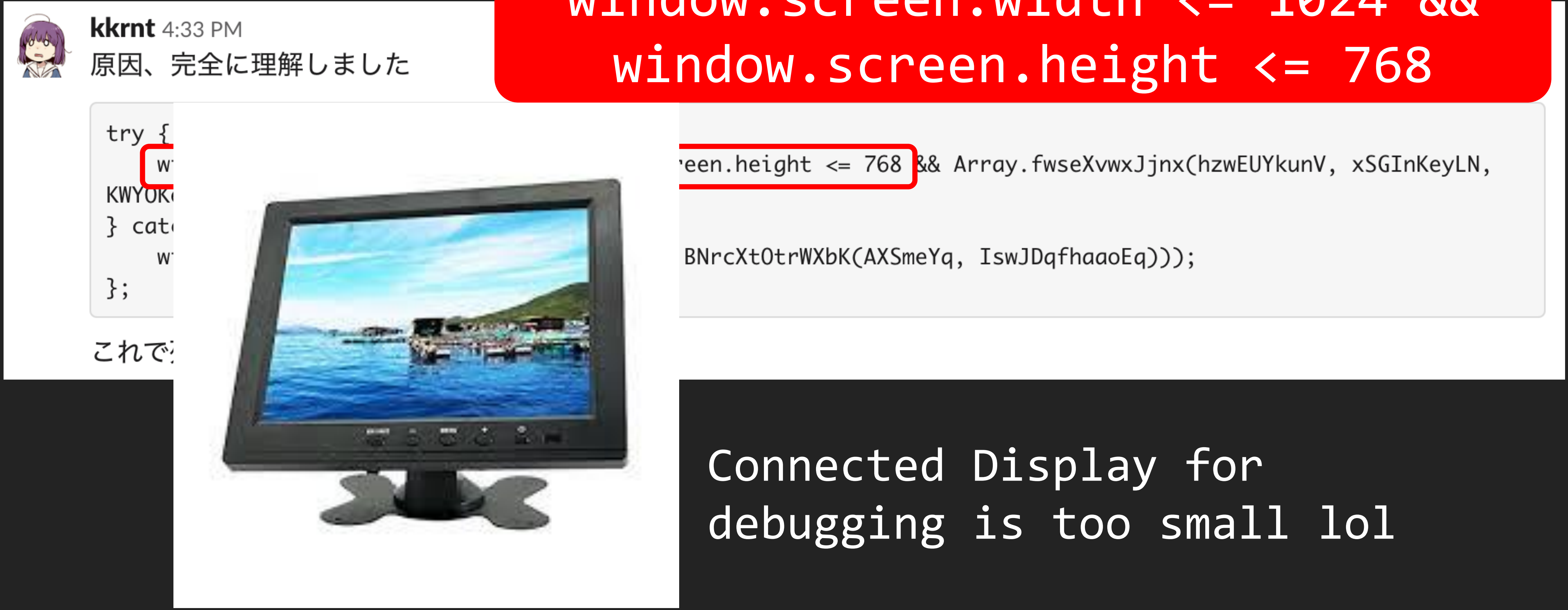
原因、完全に理解しました

```
try {
    window.screen.width <= 1024 && window.screen.height <= 768 && Array.fwseXvwxJjnx(hzwEUYkunV, xSGInKeyLN,
KWYOKeMDR);
} catch (HofRA) {
    window.location.replace(OAaXz(OYqEgOmSs, BNrcXtOtrWXbK(AXSmeYq, IswJDqfhaaoEq)));
};
```

これで死んでる

Copyright©2019 nao_sec All Rights Reserved.

Defeating Anti-Sandbox: Sandbox Detection by Display Resolution



```
window.screen.width <= 1024 &&
window.screen.height <= 768
```

kkrnt 4:33 PM

原因、完全に理解しました

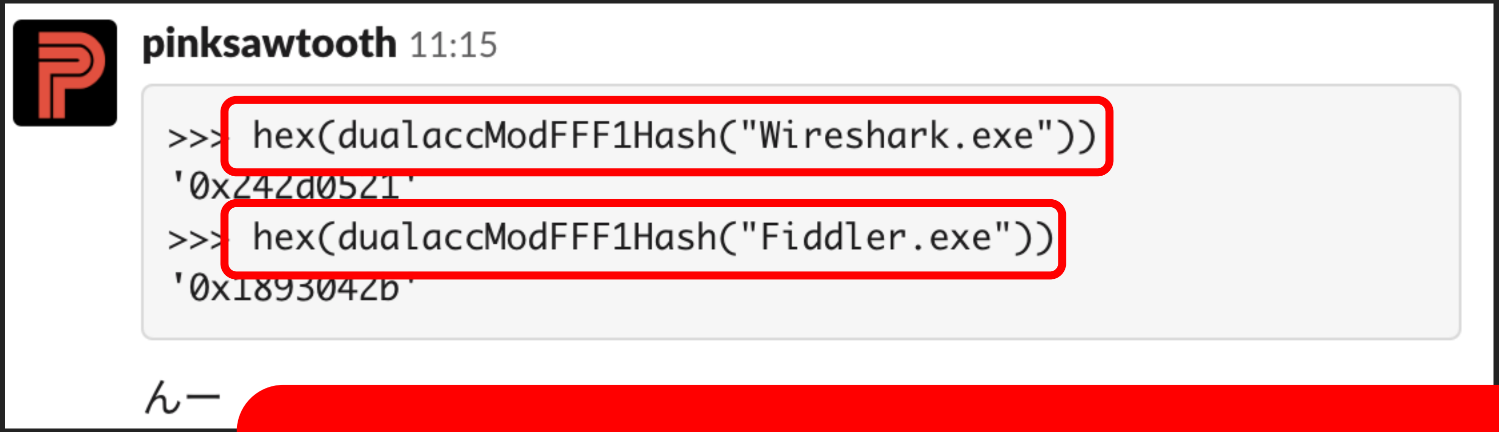
```
try {
    w                        een.height <= 768 && Array.fwseXvwxJjnx(hzwEUYkunV, xSGInKeyLN,
KWYOK
} cat
    w                        BNrcXtOtrWXbK(AXSmeYq, IswJDqfhaaoEq)));
};
```

これで

Connected Display for debugging is too small lol

Copyright©2019 nao_sec All Rights Reserved.

Defeating Anti-Sandbox: Process Detection



pinksawtooth 11:15

```
>>> hex(dualaccModFFF1Hash("Wireshark.exe"))
'0x242d0521'
>>> hex(dualaccModFFF1Hash("Fiddler.exe"))
'0x1893042b'
```

んー

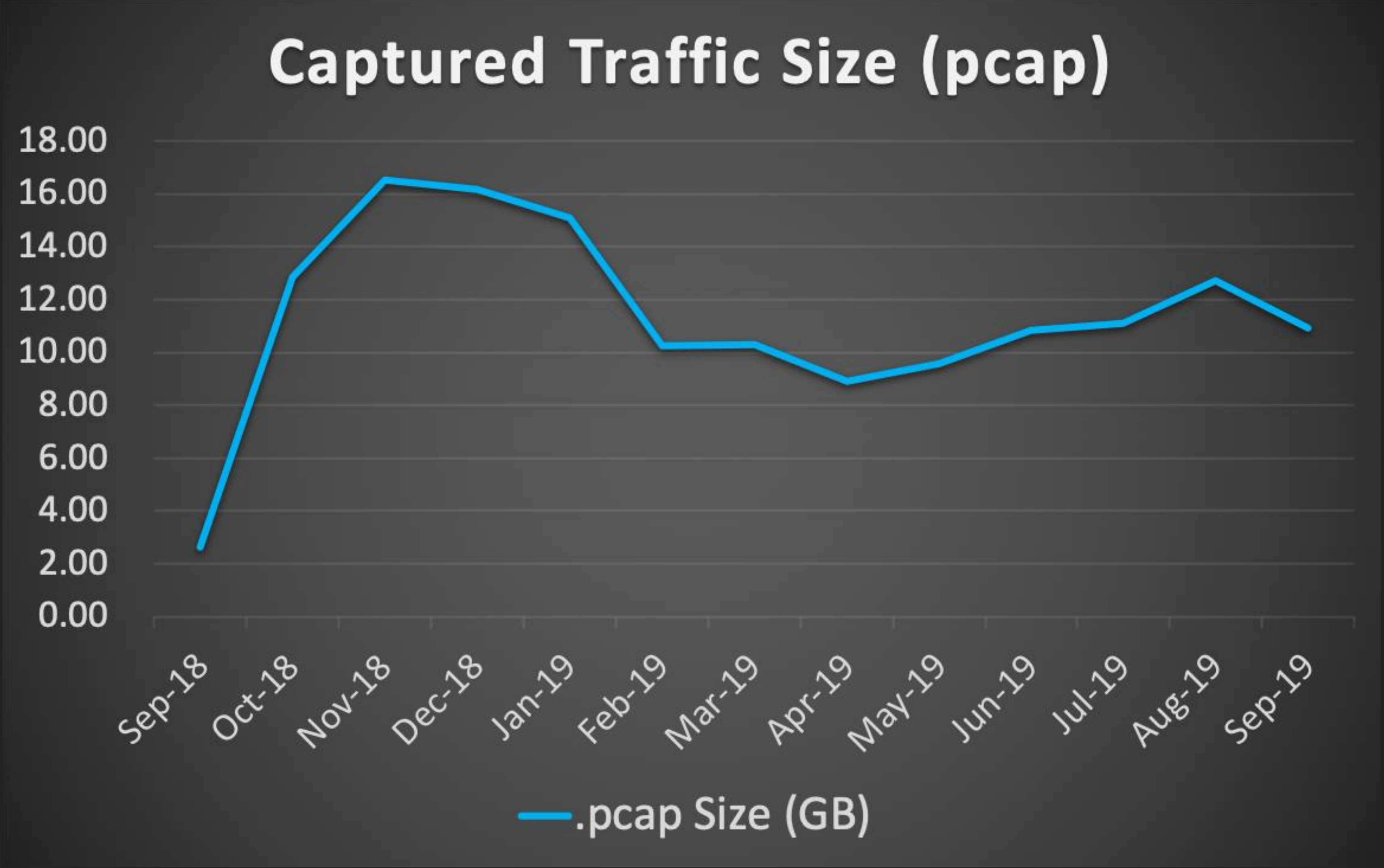
In Fallout shellcode, included hashed process name of major analysis tools

Copyright©2019 nao_sec All Rights Reserved.

Result of EK Observation by Our Platform

Copyright©2019 nao_sec All Rights Reserved.

Statistics - Crawling



147.1

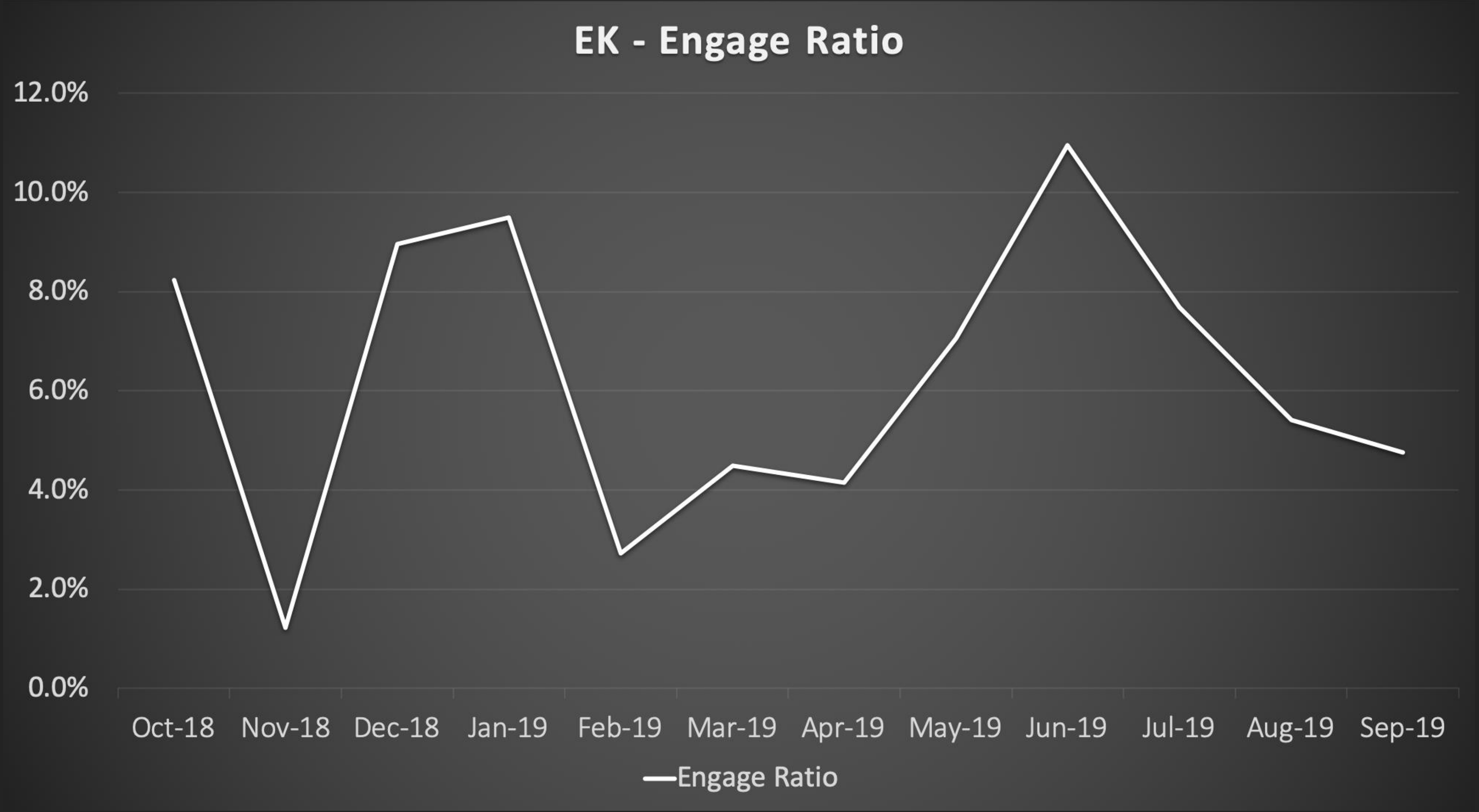
GB/Year

91,276

Crawl

Copyright©2019 nao_sec All Rights Reserved.

Statistics – Engagement Efficiency

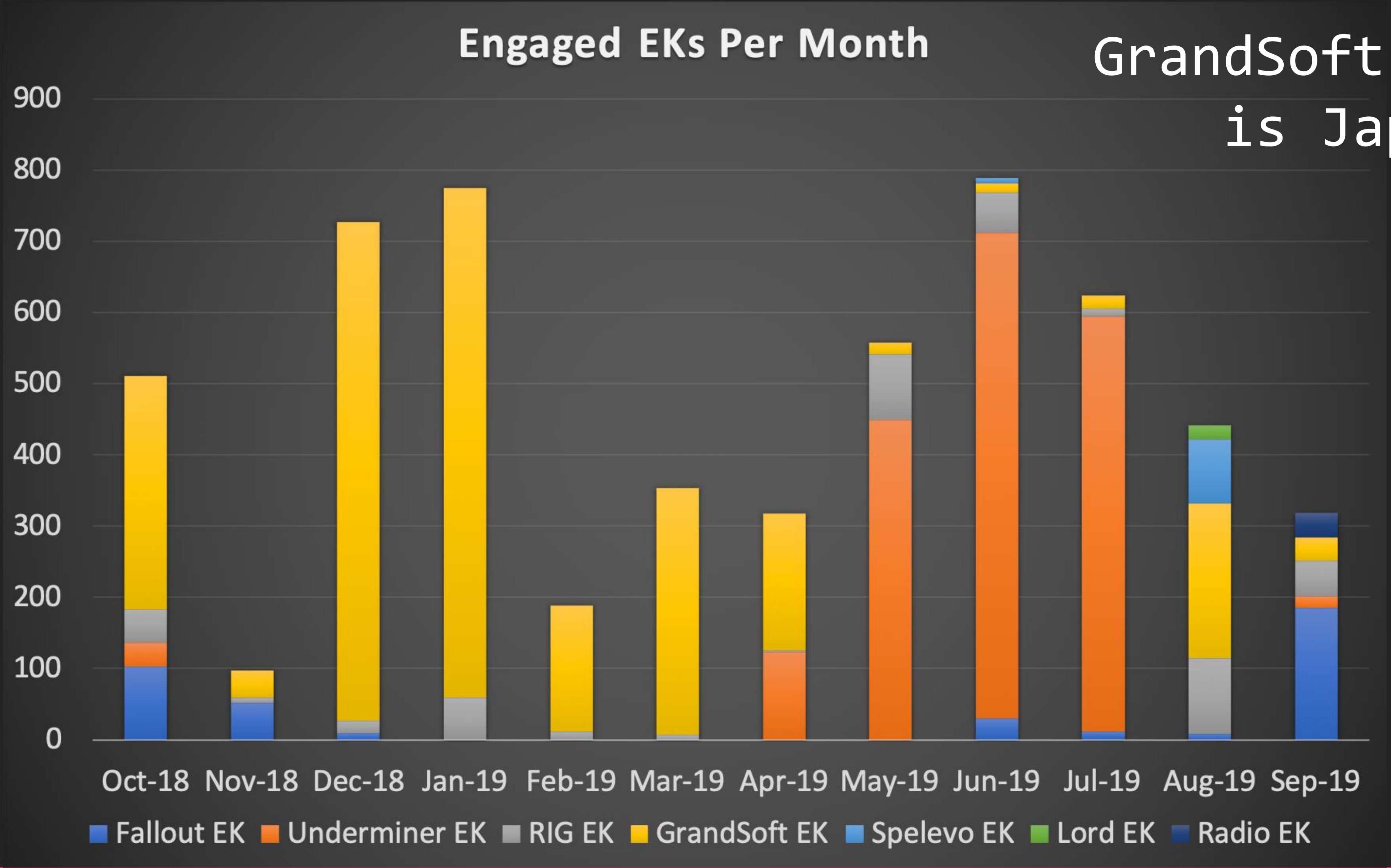


6.2%

Engage Ratio (Ave.)

Copyright©2019 nao_sec All Rights Reserved.

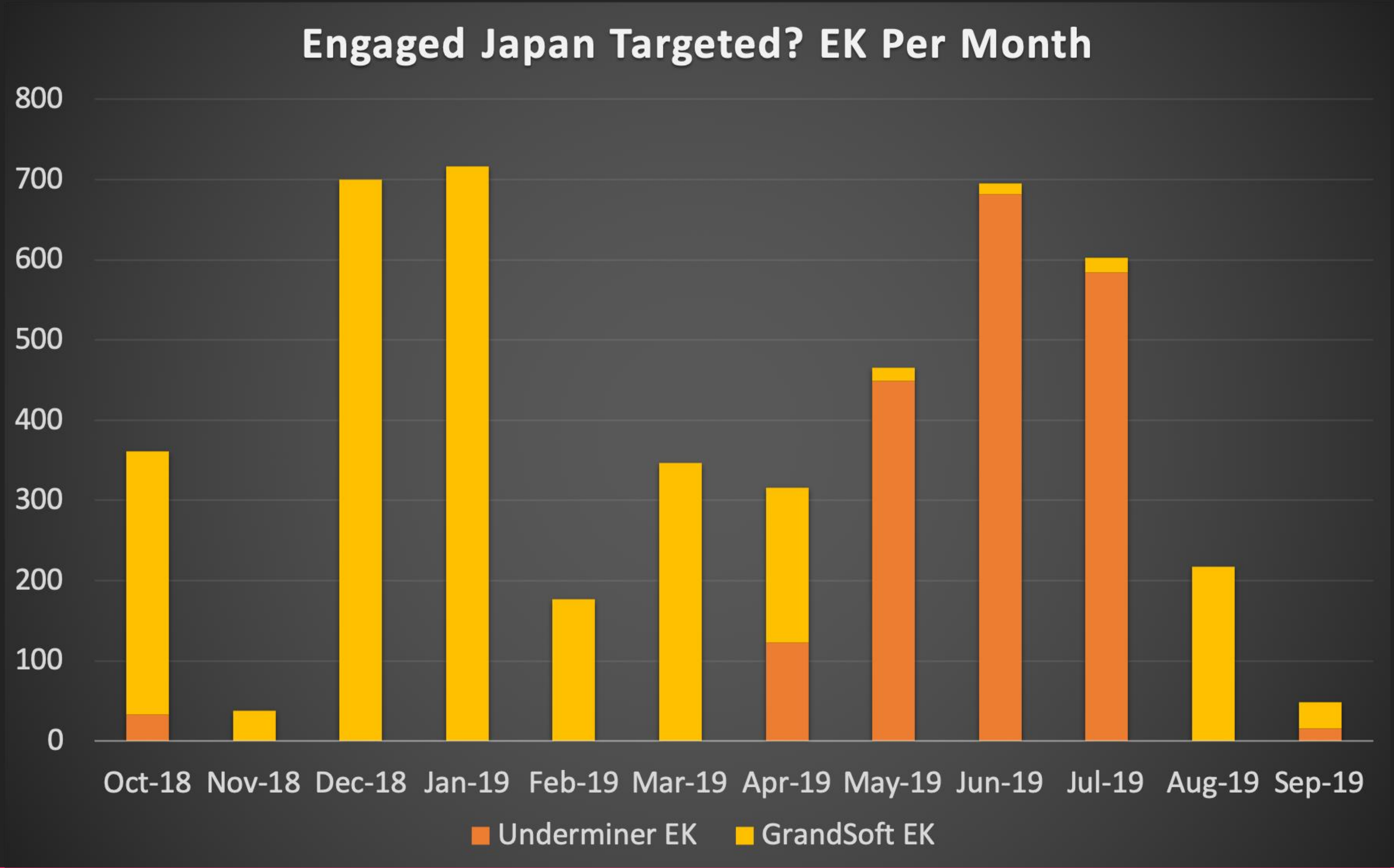
Statistics – Engaged EKs



GrandSoft mainly target is Japan and Canada

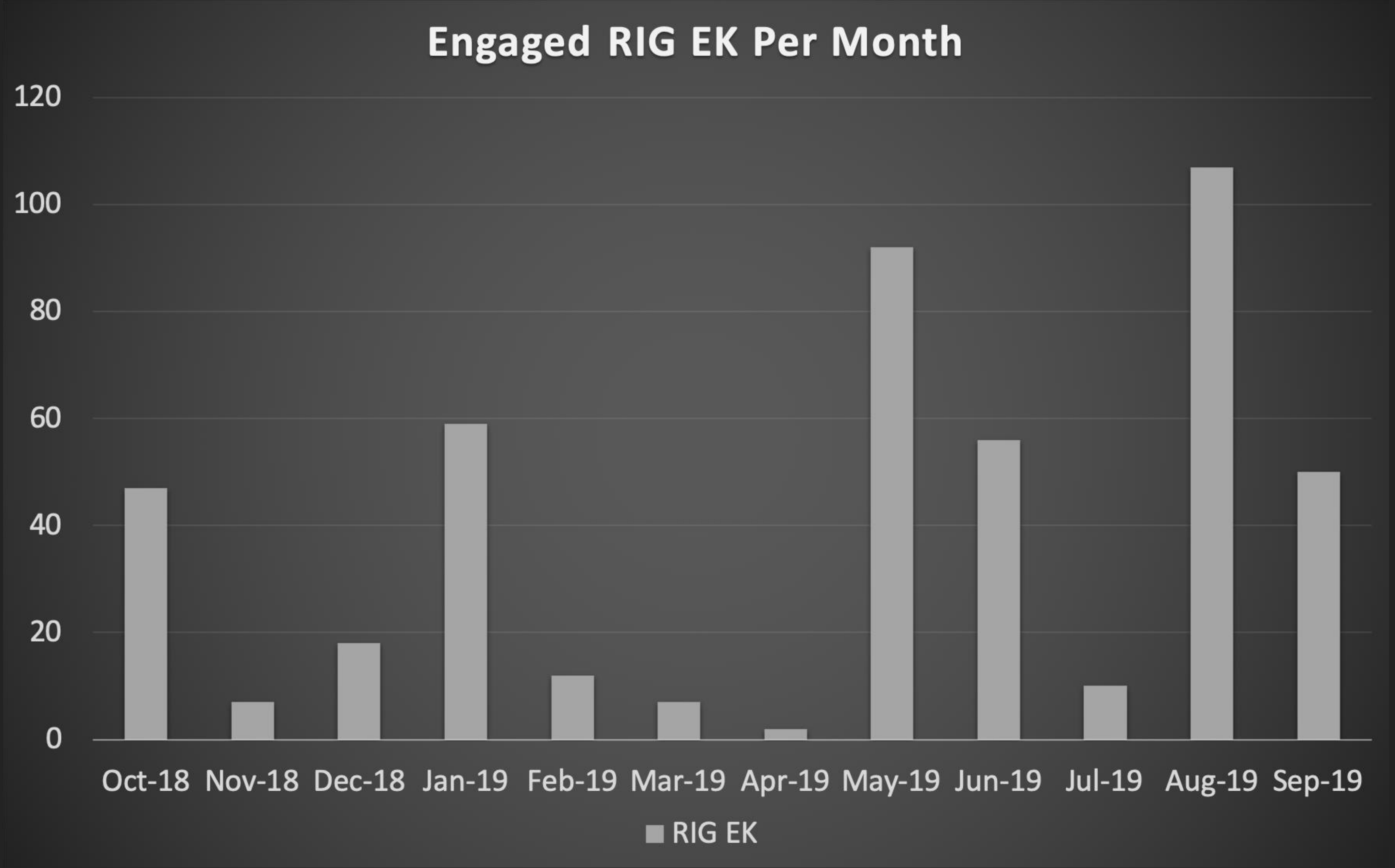
Copyright©2019 nao_sec All Rights Reserved.

Insight: Underminer EK & GrandSoft EK



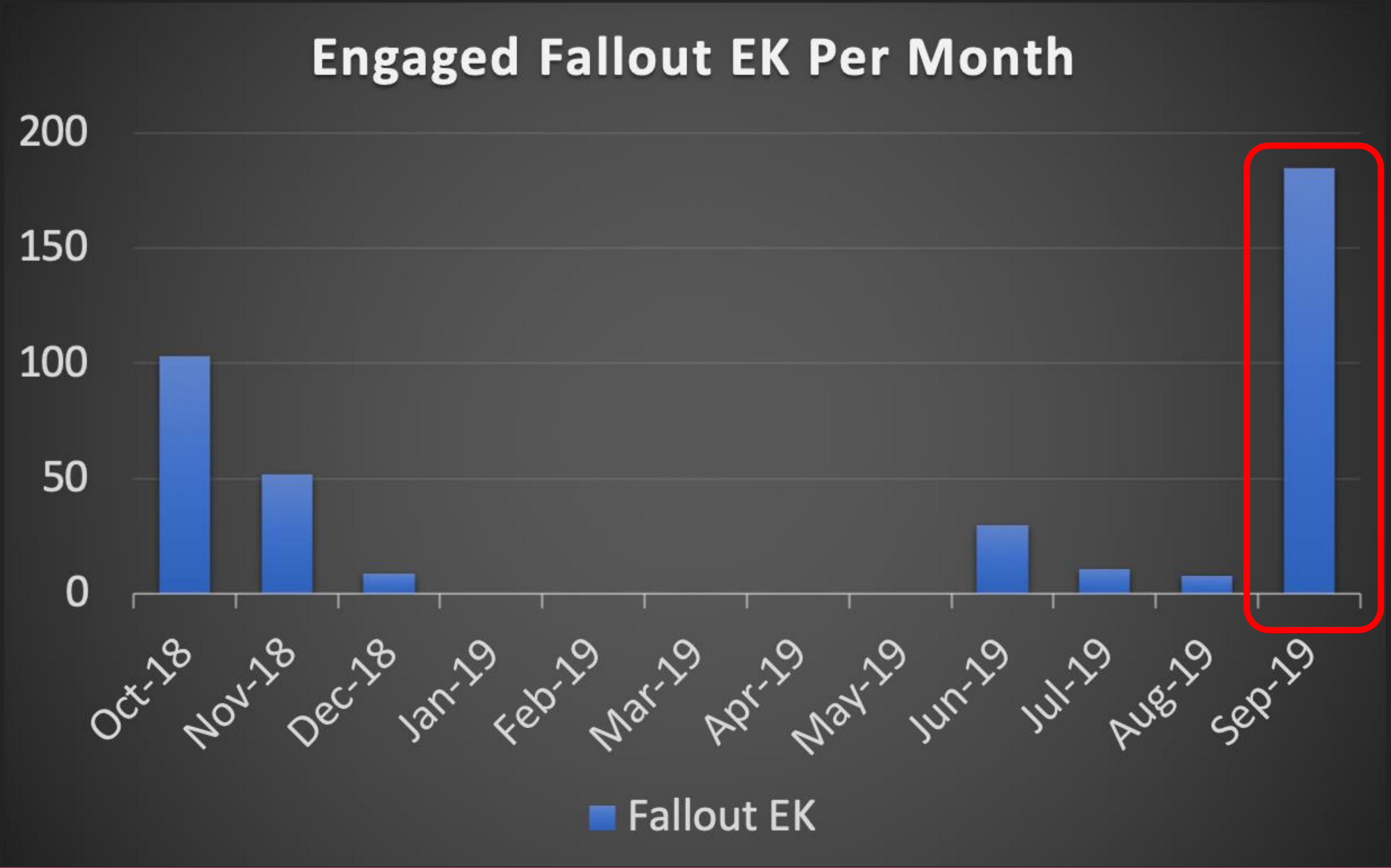
Copyright©2019 nao_sec All Rights Reserved.

Insight: RIG EK



Copyright©2019 nao_sec All Rights Reserved.

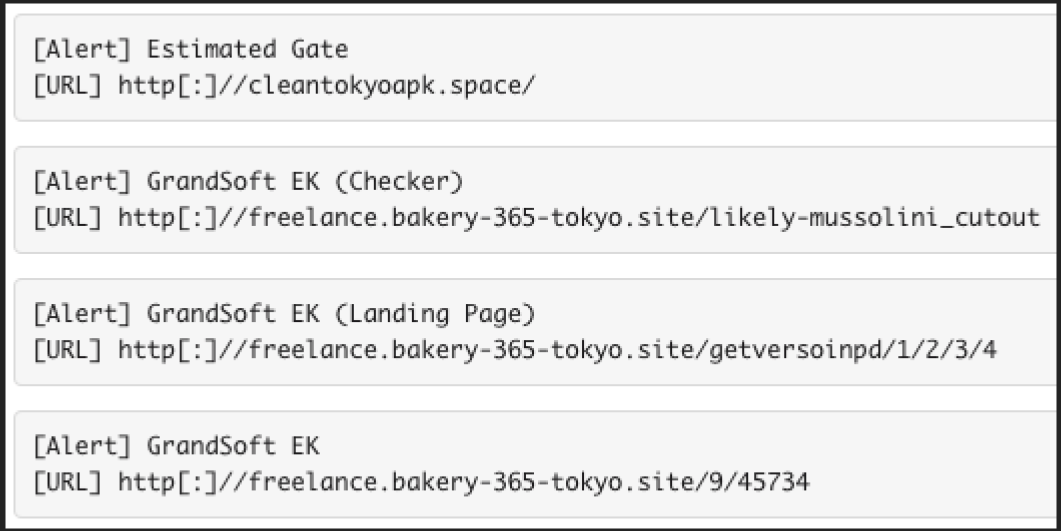
Insight: Fallout EK



Copyright©2019 nao_sec All Rights Reserved.

Discovery of New Campaigns

- **PseudoGate**
  - Observed in Japan and Canada
  - Using a Gate that looks like a legitimate website
  - Pushing Ramnit with GrandSoft Exploit Kit
  - Maybe related to Seamless campaign



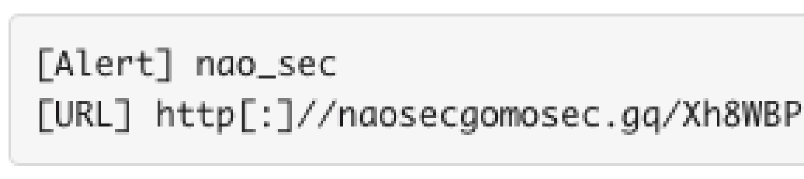
```
[Alert] Estimated Gate
[URL] http[:]//cleantokyoapk.space/

[Alert] GrandSoft EK (Checker)
[URL] http[:]//freelance.bakery-365-tokyo.site/likely-mussolini_cutout

[Alert] GrandSoft EK (Landing Page)
[URL] http[:]//freelance.bakery-365-tokyo.site/getversoinpd/1/2/3/4

[Alert] GrandSoft EK
[URL] http[:]//freelance.bakery-365-tokyo.site/9/45734
```

Copyright©2019 nao_sec All Rights Reserved.

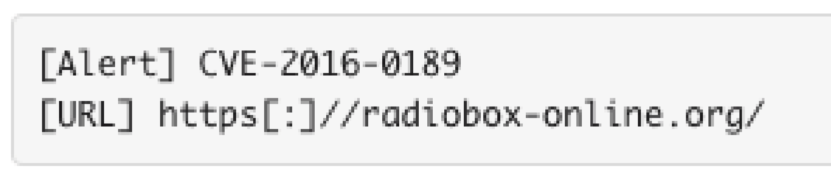
Discovery of New Exploit Kits

- **Fallout**
  - Discovered during the debugging of our system
  - Detected with “naosec” string in the domain
  - Automatic observation of all version upgrades

- **Radio**
  - The system discovered and informed us
  - Detected with CVE-2016-0189 signature



```
[Alert] nao_sec
[URL] http[:]//naosecgomosec.gq/Xh8WBP
```

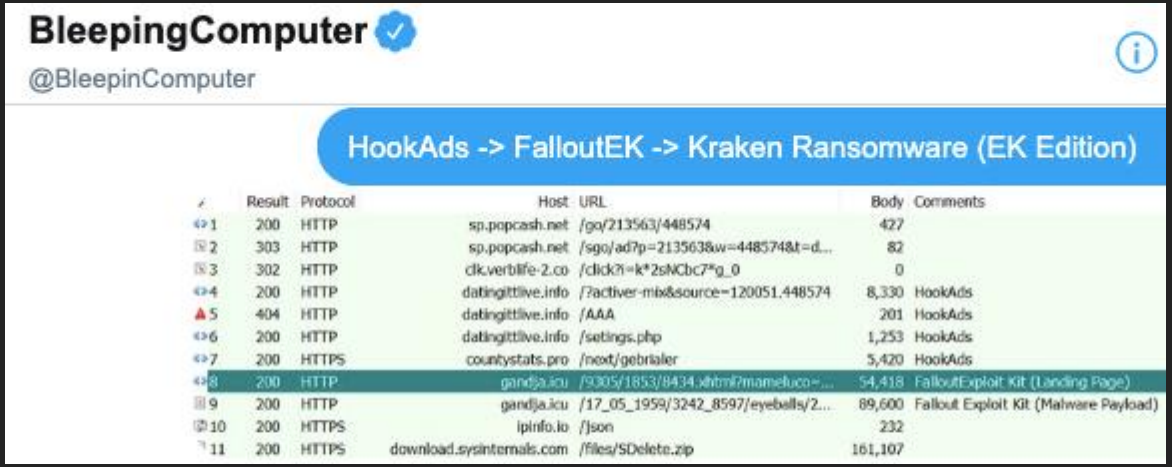


```
[Alert] CVE-2016-0189
[URL] https[:]//radiobox-online.org/
```

Copyright©2019 nao_sec All Rights Reserved.

Discovery of New Malwares

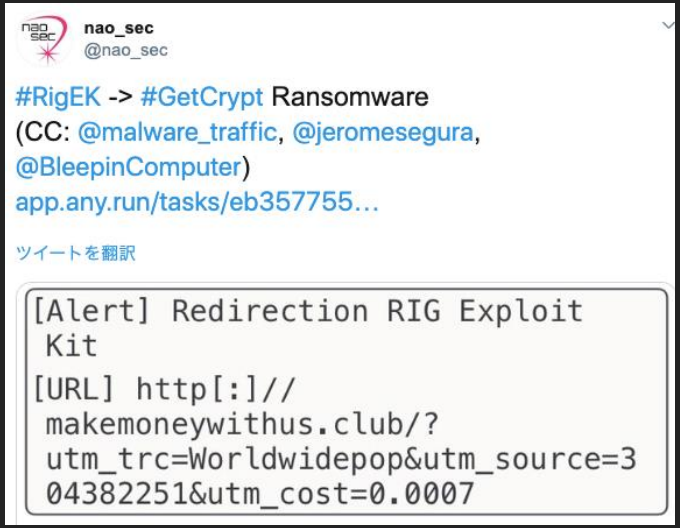
- Kraken Cryptor
- GetCrypt
- Buran
- SystemBC



BleepingComputer
@BleepinComputer

HookAds -> FalloutEK -> Kraken Ransomware (EK Edition)

#	Result	Protocol	Host	URL	Body	Comments
1	200	HTTP	sp.popcash.net	/go/213563/448574	427	
2	303	HTTP	sp.popcash.net	/sgo/ad?p=213563&w=448574&t=d...	82	
3	302	HTTP	clk.verblife-2.co	/click?i=k*2sNCbc7*g_0	0	
4	200	HTTP	datingittlive.info	/?activer-mix&source=120051.448574	8,330	HookAds
5	404	HTTP	datingittlive.info	/AAA	201	HookAds
6	200	HTTP	datingittlive.info	/setings.php	1,253	HookAds
7	200	HTTPS	countystats.pro	/next/gebrialer	5,420	HookAds
8	200	HTTP	gandja.icu	/9305/1853/8434.xhtml?mameluco=...	54,418	FalloutExploit Kit (Landing Page)
9	200	HTTP	gandja.icu	/17_05_1959/3242_8597/eyeballs/2...	89,600	Fallout Exploit Kit (Malware Payload)
10	200	HTTPS	ipinfo.io	/json	232	
11	200	HTTPS	download.sysinternals.com	/files/SDelete.zip	161,107	

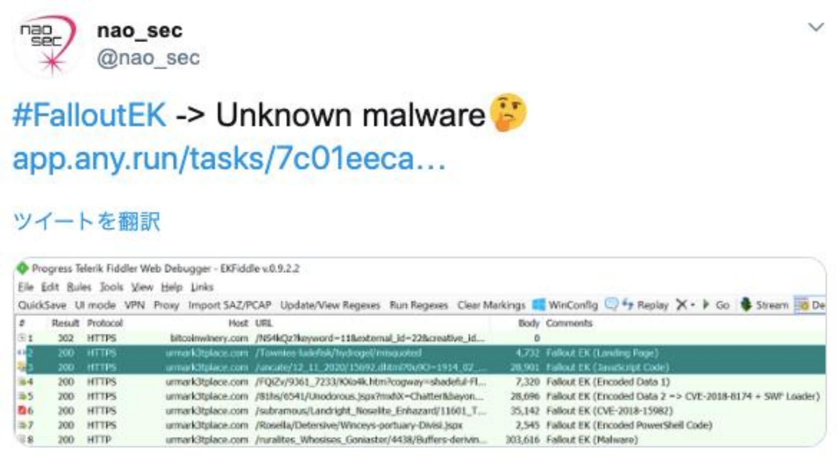


nao_sec
@nao_sec

#RigEK -> #GetCrypt Ransomware
(CC: @malware_traffic, @jeromesegura, @BleepinComputer)
app.any.run/tasks/eb357755...

ツイートを翻訳

```
[Alert] Redirection RIG Exploit
 Kit
[URL] http[:]//
 makemoneywithus.club/?
 utm_trc=Worldwidepop&utm_source=3
 04382251&utm_cost=0.0007
```



nao_sec
@nao_sec

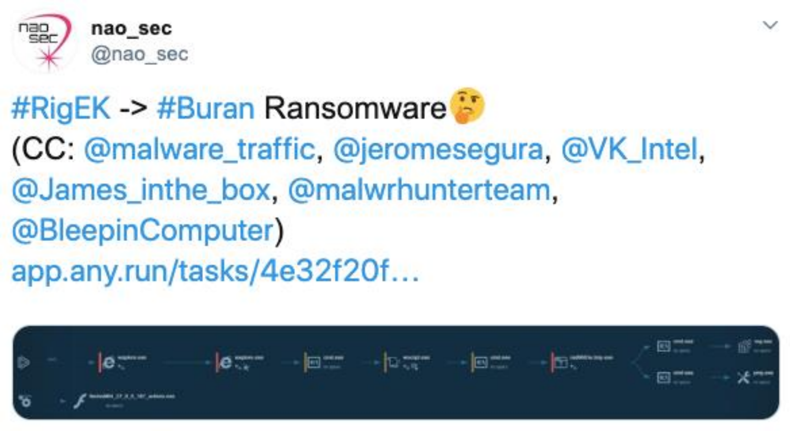
#FalloutEK -> Unknown malware🤔
app.any.run/tasks/7c01eeca...

ツイートを翻訳

Progress Telerik Fiddler Web Debugger - EKFiddle v.0.9.2.2

File Edit Rules Tools View Help Links
QuickSave UI mode VPN Proxy Import SAZ/PCAP Update/View Regexes Run Regexes Clear Markings WinConfig Replay Go Stream De

#	Result	Protocol	Host	URL	Body	Comments
1	302	HTTPS	bitcoinwinery.com	/NS4kQz?keyword=11&external_id=22&creative_id...	0	
2	200	HTTPS	urmark3tplace.com	/Townies-ladefisk/hydrogel/misquoted	4,732	Fallout EK (Landing Page)
3	200	HTTPS	urmark3tplace.com	/uncate/12_11_2020/15692.dhtml?ou9O=1914_02_...	28,901	Fallout EK (JavaScript Code)
4	200	HTTPS	urmark3tplace.com	/FQiZv/9361_7233/Kklo4k.htm?cogway=shadeful-Fl...	7,320	Fallout EK (Encoded Data 1)
5	200	HTTPS	urmark3tplace.com	/81hs/6541/Unodorous.jspx?mxfiX=Chatter&bayon...	28,696	Fallout EK (Encoded Data 2 => CVE-2018-8174 + SWF Loader)
6	200	HTTPS	urmark3tplace.com	/subramous/Landright_Noselite_Enhazard/11601_T...	35,142	Fallout EK (CVE-2018-15982)
7	200	HTTPS	urmark3tplace.com	/Rosella/Detersive/Winceys-portuary-Divisi.jspx	2,545	Fallout EK (Encoded PowerShell Code)
8	200	HTTP	urmark3tplace.com	/nuralites_Whosises_Goniaster/4438/Buffers-dervin...	303,616	Fallout EK (Malware)



nao_sec
@nao_sec

#RigEK -> #Buran Ransomware🤔
(CC: @malware_traffic, @jeromesegura, @VK_Intel, @James_inthe_box, @malwrhunterteam, @BleepinComputer)
app.any.run/tasks/4e32f20f...

Copyright©2019 nao_sec All Rights Reserved.

Weak Point of Our System

- **Manual research can be more sensitive**
  - OPSEC fail
    - Leaking info
      - EK API
      - Directory listing

- Finding a new one is not easy
  - Need to combine other logic

- **Observation environmet**
  - Windows version, IP geolocation

Copyright©2019 nao_sec All Rights Reserved.

Our Contributions

- **The number of times our research has been referred**
  - More than 40 public reports from various organizations

- **Dataset for academic research in Japan**

Copyright©2019 nao_sec All Rights Reserved.

Conclusion

Copyright©2019 nao_sec All Rights Reserved.

Conclusion

- Introducing the design, effectiveness and practical use cases of an automated active analysis platform

- We show the changes to the threat landscape by using the results from our platform

- We talked about how we continue to discover and track new attack campaigns and Exploit Kits, such as the Fallout and Radio Exploit Kit

Copyright©2019 nao_sec All Rights Reserved.

Any Questions?

Twitter: @nao_sec
Email: info@nao-sec.org

Copyright©2019 nao_sec All Rights Reserved.