Japan Security Analyst Conference 2018

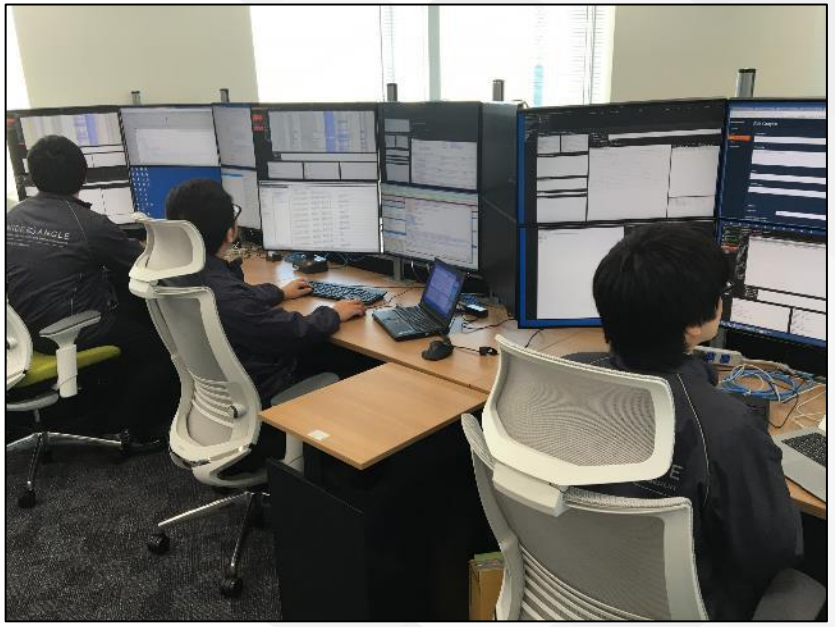
RIGエクスプロイトキットの調査

NTTセキュリティ・ジャパン株式会社
幾世 知範

NTT Security

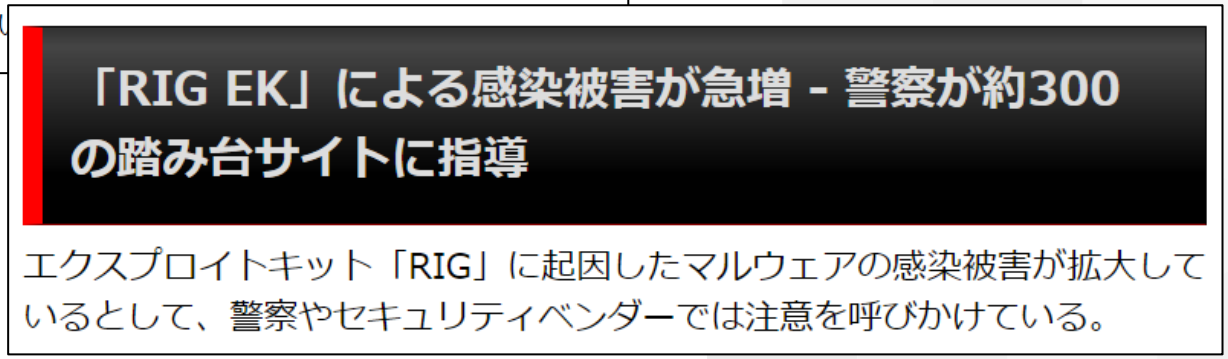
自己紹介

- SOCのアナリスト
  - –24/365体制での監視・分析
  - –ホワイトペーパーの執筆
    - **RIGエクスプロイトキットの調査**
    - 北朝鮮関連サイトを踏み台とした水飲み場型攻撃の調査
    - マルウェアURSNIFの解析



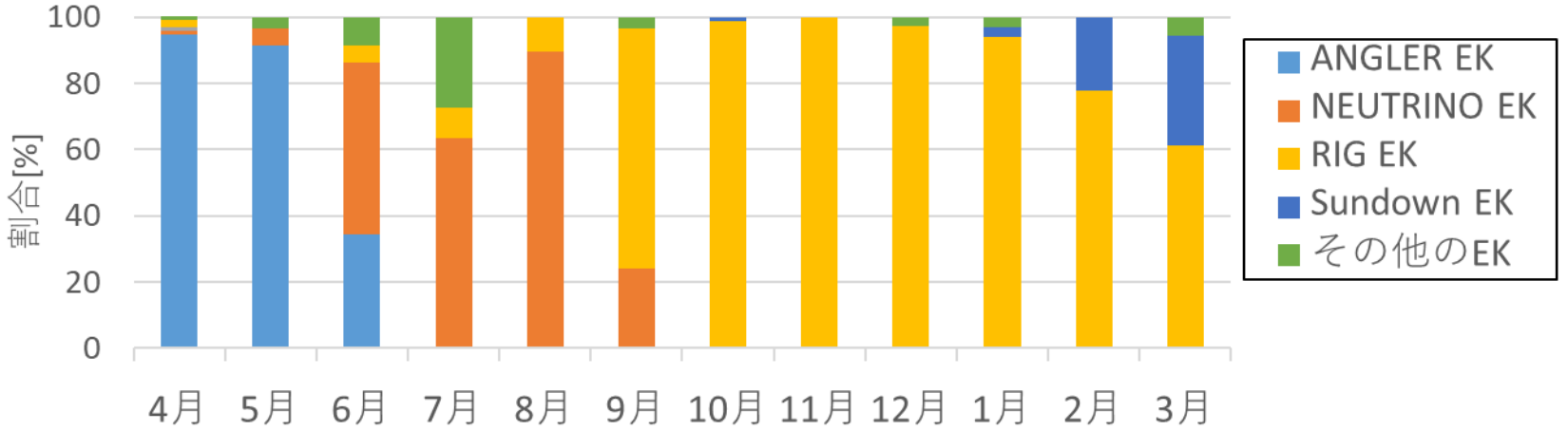
RIG EKを用いた攻撃が多発（していた）

- セキュリティベンダーや警察が注意喚起や対策を実施[1][2]



SOCでの観測状況

- RIG EK（RIG 4.0）を用いた攻撃は2016年9月から増加
  - –現在はドライブバイダウンロード攻撃自体が下火



通知したインシデントにおけるエクスプロイトキットの内訳
（2016年4月～2017年3月）

NTT Security

SOCアナリストの調査観点

調査目的	調査項目の例
攻撃検知	ドメイン/IPアドレス URLパターン 攻撃コードの特徴
攻撃受けた場合の影響把握	悪用される脆弱性 感染するマルウェア
全体像の把握	背後関係

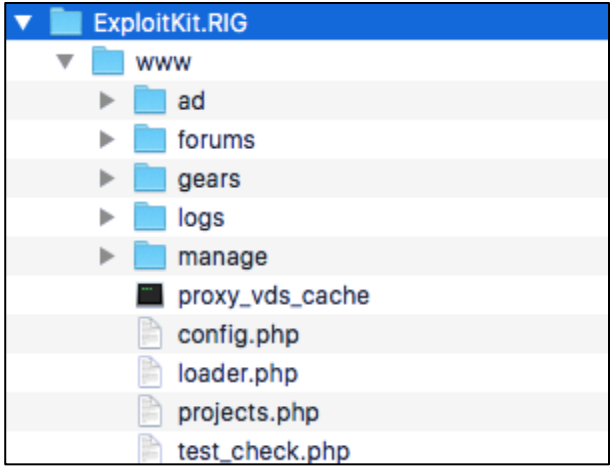
※下線付きの項目について調査方法を紹介

目次

- エクスプロイトキットの概要
- RIGエクスプロイトキットの調査方法
  - 攻撃サイトドメイン/IPアドレスの収集
  - 悪用される脆弱性の確認
  - 背後関係の調査

エクスプロイトキット（EK : Exploit Kit）

- パッケージ化された攻撃用コード群
  - 本プレゼンではドライブバイダウンロード攻撃に利用されるものを指す



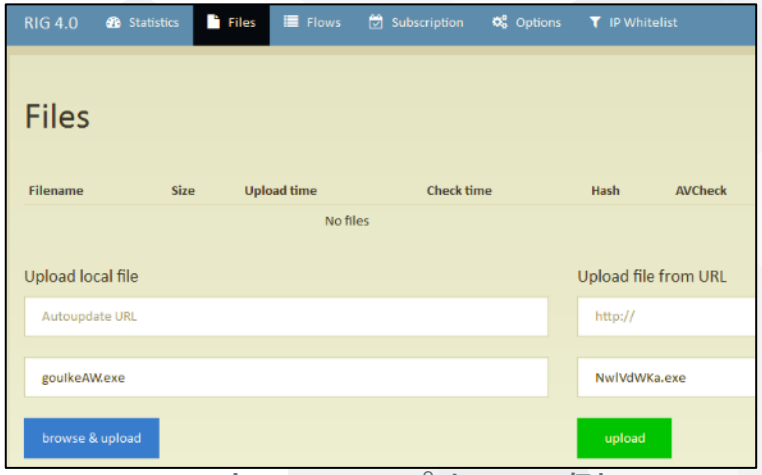
サーバプログラム

```
sc[e]=ah[e]._vgRuntimeStyle;
for(e=0;e<StringHex2Int("0x400");e++){
sc[e].rotation,e==StringHex2Int("0x300")&&
  35 36 37 38 39 40 41 42 43 44");
}
le=gm.dashstyle.array.length;
}
try{
  gm.dashstyle.array.length=-1
}catch(a){
  return!1
}
```

攻撃コード
（脆弱性を悪用）

EKの販売形態

- **サービス（主流）**
  - –利用者にコントロールパネルを提供
    - 統計情報閲覧やマルウェア登録が可能
  - –脆弱性を悪用してマルウェアを配布
  - –利用期間に応じた価格設定
- プログラムコード



コントロールパネルの例

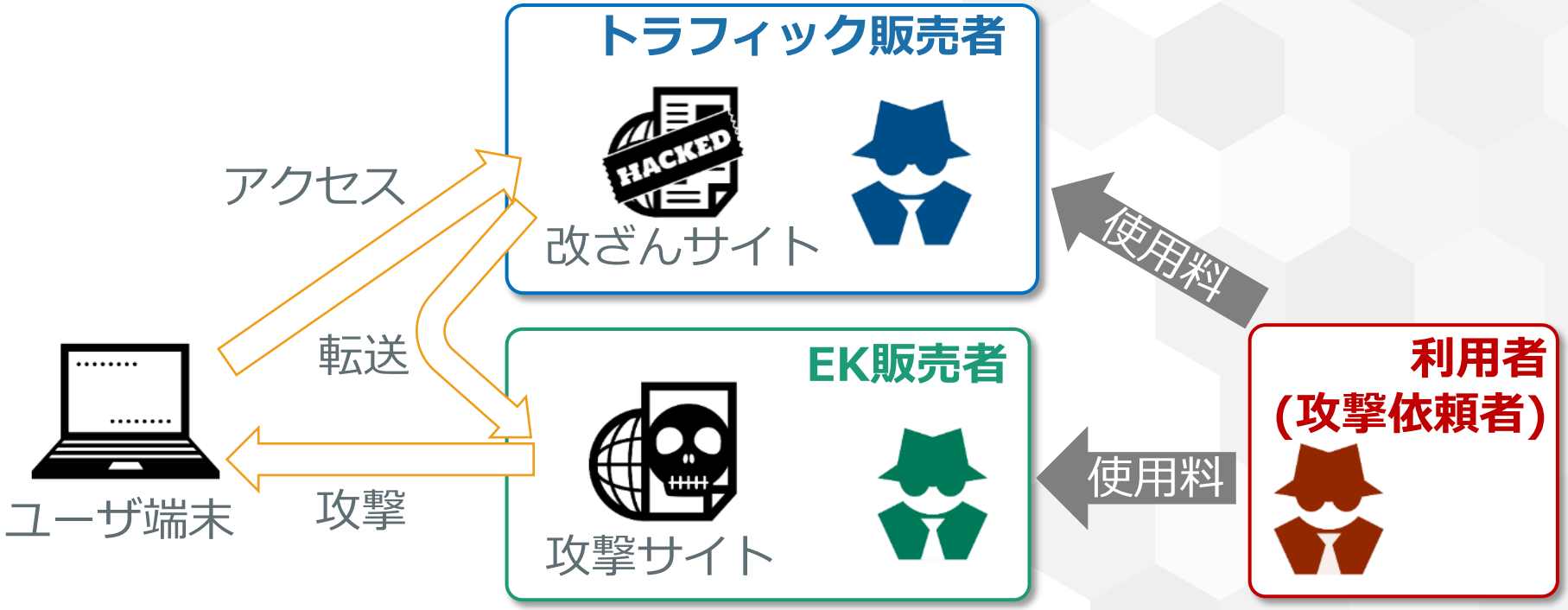
価格の提示例

NTT Security

EKへの誘導

- いわゆるキャンペーン
  - EI Test
  - Seamless
  - Fobos
  - など
- トラフィックという名称で売買
  - 誘導回数/対象に応じた価格設定

EKを用いた攻撃の役割分担



目次

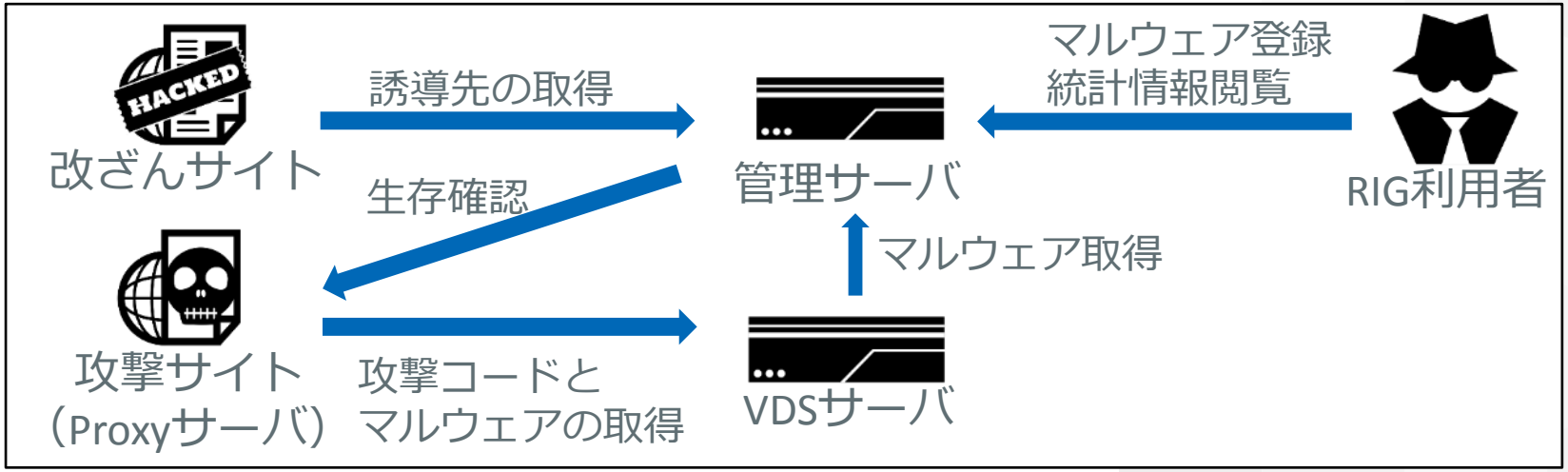
- エクスプロイトキットの概要
- RIGエクスプロイトキットの調査方法
  - –攻撃サイトドメイン/IPアドレスの収集
  - –悪用される脆弱性の確認
  - –背後関係の調査

攻撃サイトドメイン/IPアドレスの収集方法

- OSINT
- 実ネットワークの監視
  - –IDS/IPS/Sandbox
- ハニーポット
  - –Webクライアント型：Web空間を巡回
  - –Webサーバ型：改ざん内容（誘導先）の監視
- EKのサーバ側に実装された機能の利用

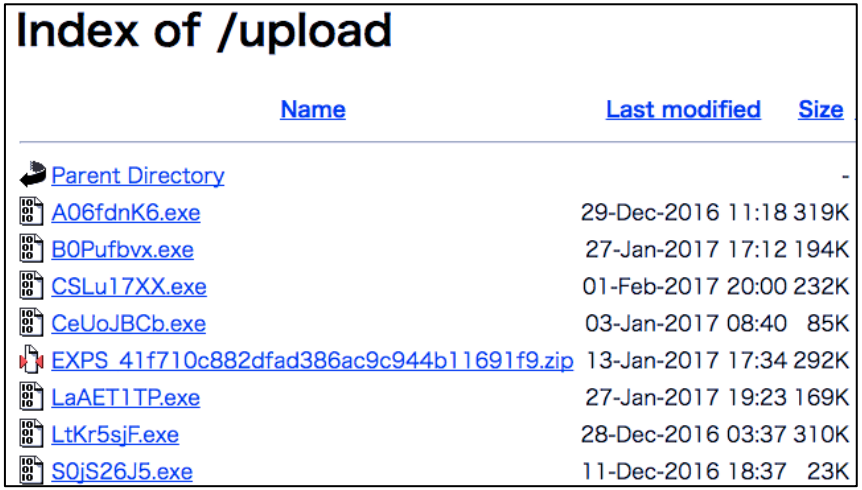
RIG 2.0のサーバ側機能[3][4]

- 登録されたマルウェアを配信
- 攻撃サイトの一覧の管理（生存確認含む）



RIG 4.0のサーバ側機能（1）

- RIG 2.0と同様にマルウェアを管理
  - –オープンディレクトリになっていたことが知られている



Index of /upload

Name	Last modified	Size
Parent Directory		-
A06fdnK6.exe	29-Dec-2016 11:18	319K
B0Pufbvx.exe	27-Jan-2017 17:12	194K
CSLu17XX.exe	01-Feb-2017 20:00	232K
CeUoJBCb.exe	03-Jan-2017 08:40	85K
EXPS_41f710c882dfad386ac9c944b11691f9.zip	13-Jan-2017 17:34	292K
LaAET1TP.exe	27-Jan-2017 19:23	169K
LtKr5sjF.exe	28-Dec-2016 03:37	310K
S0jS26J5.exe	11-Dec-2016 18:37	23K

管理用サーバ上のuploadディレクトリ

uploadディレクトリのコンテンツへの言及

RIG 4.0のサーバ側機能（2）

- 投影のみ

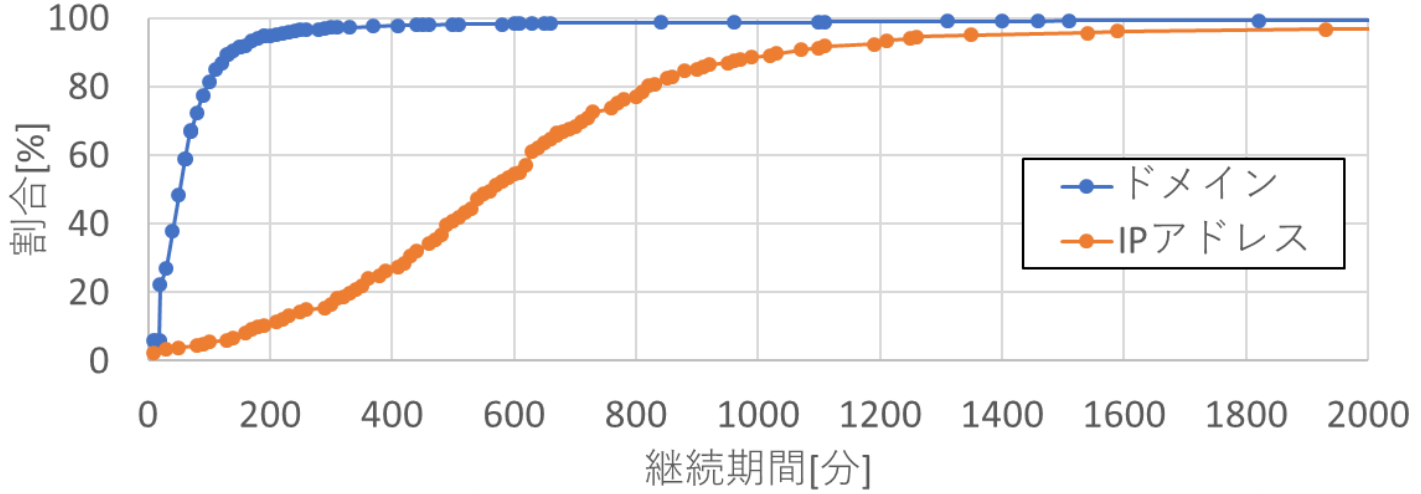
観測結果の比較

- 生存確認機能は他の方法で観測したドメインを包含

	実ネットワーク	クローラ	サーバの生存確認機能
2017/02/07 20:30	-	one.jakesflowers[.]com	indianoshop[.]tk one.jakesflowers[.]com
2017/02/07 20:40	one.jakesflowers[.]com	one.jakesflowers[.]com	indianoshop[.]tk one.jakesflowers[.]com
2017/02/07 20:50	-	trend.padrecam[.]com	indianoshop[.]tk trend.padrecam[.]com
2017/02/07 21:00	-	trend.padrecam[.]com	indianoshop[.]tk trend.padrecam[.]com

ドメイン/IPアドレスの傾向（2017年1月～3月）

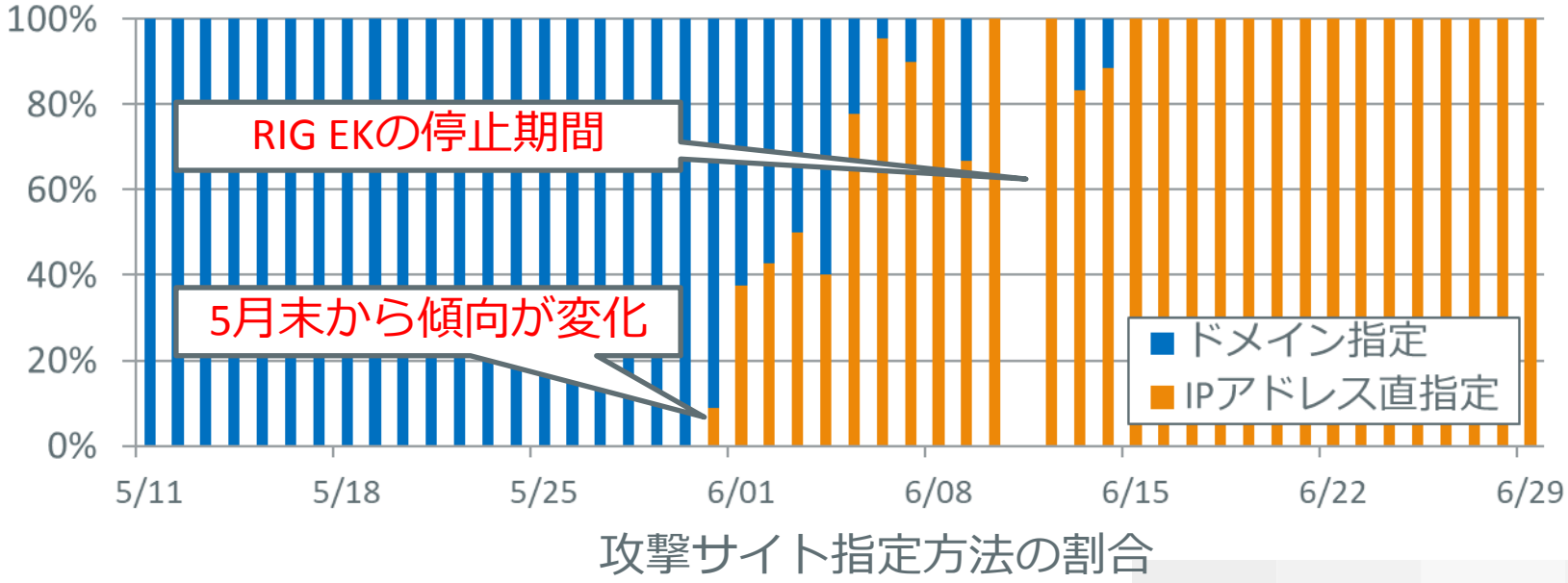
- 1か月あたり約700ドメインを利用
- ドメイン自体よりも紐づくIPアドレスの利用期間が長い



利用期間の累積グラフ（2017/1 ～ 2017/3に収集したデータ）

ドメイン/IPアドレスの傾向（2017年6月～）

- ドメイン指定からIPアドレス直指定に変化



NTT Security

RIG EK以外のサーバ側機能（Eris EK）

- 攻撃サイトと思しきURLとコンテンツを管理
  - –/rotator（controllers/Flow.php)
  - –/landing (controllers/landing.php)

<head><title>5907bdf8490a2</title><script>window.onload = function() {eval(fun
ction(p,a,c,k,e,d){e=function(c){return(c<a?'':e(parseInt(c/a)))+((c=c%a)>35?String.
...
<form id="frm" name="frm" action="**http://178.62.90[.]157//177872/5907bdf84
a158**" method="POST"><input type="text" value="" name="A5907b" hidden style

landingのレスポンス（ブラウザのプラグイン確認）

➡サーバ側の機能を利用した調査は他のEKにおいても効果有

目次

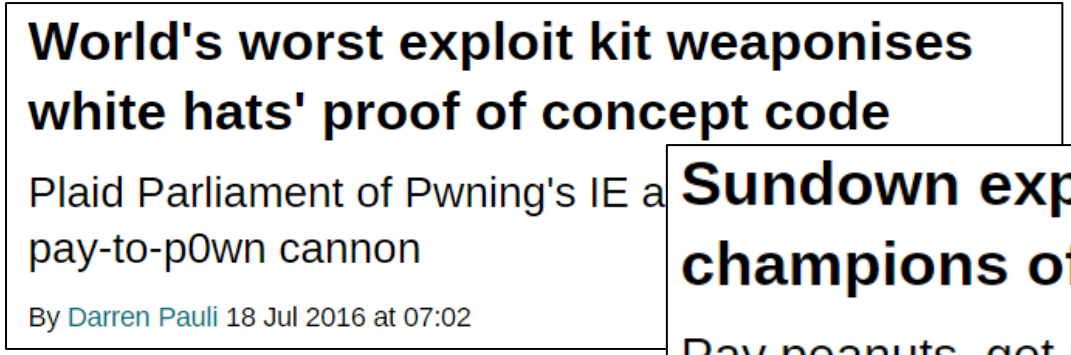
- エクスプロイトキットの概要
- RIGエクスプロイトキットの調査方法
  - 攻撃サイトドメイン/IPアドレスの収集
  - 悪用される脆弱性の確認
  - 背後関係の調査

悪用される脆弱性の確認手順

1. 攻撃コードの取得
   - –実ネットワークやハニーポット
2. 攻撃コードの可読性の向上
   - –JavaScriptコードの難読化解除 など
3. 悪用される脆弱性の特定
   a. デバッガ、逆アセンブラを利用した解析
   b. 過去の攻撃コードとの類似性を確認

攻撃コードの流用

- EK作成者は既存の攻撃コードを流用して開発コストを削減
  - セキュリティ研究者の成果[5]
  - 他のEKの攻撃コード[6]



RIG EKにおける攻撃コードの流用

- Angler EKのコードを改変して利用していることを確認
  - –部分的に書き換えて利用しているため使用しないコードが含まれる

```
for (f = 0;f < a.length;f += 8){
      c[0] = Il1Iwa(a.substring(f, f + 4));
      c[1] = Il1Iwa(a.substring(f + 4, f + 8));
      g = c;
      for (var h = g[0], k = g[1], l = 84941944608;0 != l;){
        k -= (h << 4 ^ h >>> 5) + h ^ l + d[l >>> 11 & 3],
        l -= 2654435769, h -= (k << 4 ^ k >>> 5) + k ^ l + d[l & 3];
      }
      g[0] = h;
      g[1] = k;
      e += Il1Ixa(c[0]) + Il1Ixa(c[1]);
    }
```

RIG EKの攻撃コードに残るXTEAの実装（RIG EKでは未使用）

RIG EKが悪用する脆弱性の特定

- 現状では文字列とコード構造の特徴から特定可能

```
try{
    gm.dashstyle.array.length=-1;
}catch(a){
```

CVE-2013-2551[7]

```
Function SmuggleFag                                    VBScript
    aw.ZeroineL()
    Dim i
    For i = 0 To k3
    y(i) = Mid(x, 1, k2*12)
    Next
End Function
```

```
var o;                                                 JavaScript
o = { "valueOf": function (){
          SmuggleFag();
          return 1;
       }
     };
setTimeout(function(){ProtectMe(o);}, 50);
```

```
Il1I4.prototype.yc = function(a){
    if (!a.ma(!1)){
      throw new Error(JSON);
    }
    a.kb(!1);
    a.ib(!1);
    JSON[“stringify”](this.Pc, this.uc);
    a.ob(!1);
    CollectGarbage();};
```

CVE-2015-2419[8]

CVE-2016-0189[9]

目次

- エクスプロイトキットの概要
- RIGエクスプロイトキットの調査方法
  - –攻撃サイトドメイン/IPアドレスの収集
  - –悪用される脆弱性の確認
  - –背後関係の調査

EK売買の大まかな流れ

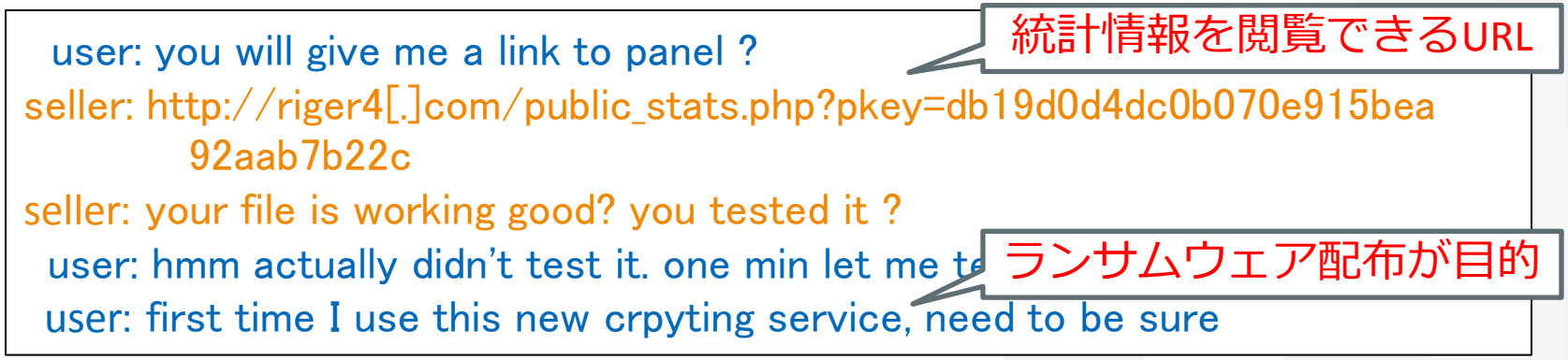
1. 販売者：特徴や価格、連絡先を書いたスレッドを作成
2. 利用者：掲示板に記載の連絡先にコンタクトして購入
   –XMPPクライアントやSkype, フォーラムのDMなどを利用
3. 販売者：EKの設定を投入

背後関係の調査方法

- サーバ側のデータとソースコードを読む
  - –RIG 2.0のようにサーバのダンプが公開された場合にのみ実施可能
- EK販売者から情報を収集
  - –公開されている会話ログの確認
    - - セキュリティ研究者が調査結果を公開
    - - EKの購入者がはらいせに公開
  - –直接コンタクト
    - - XMPPやSkypeなどのメッセンジャーを利用

公開されている会話ログの例

- 販売形態や価格、購入目的などを確認可能
  - –有効性を示すため統計情報を開示している場合有



会話ログの例（一部編集）

会話ログの検索

- フォーラムの検索機能や検索エンジンを使用
- 会話に出現しやすいワードを検索
  - 公開統計情報のURL
    - RIG EKの場合はpublic_stats.php
  - コントロールパネルのドメイン名
    - RIG 4.0の場合はrigek[.]com, rigpriv[.]com
  - など

公開されている会話ログの例（RIG 4.0）

- EK利用者がトラフィックを購入 → 従来と同じ役割分担

```
traffic user  : start soon?
traffic seller: now bro
traffic user  : k
traffic user  : still nothing
traffic seller: now go traffic
traffic user  : i didnt got anything
traffic user  : http://rigpriv[.]com/public_stats.php?pkey=ec36f40723a6d142c0b4a
                87410df058e
```

会話ログの抜粋（一部編集）

【参考】RIG 4.0の公開統計情報

- アクセス元
  - –OS
  - –ブラウザ
  - –国
- 悪用する脆弱性
- 攻撃成功率
- 設置ファイル

Attack type

Name	Exploits	Percent
silver	16	57.1 %
flash	9	32.1 %
msie-2551	2	7.1 %
msie-2419	1	3.6 %

悪用を試みた脆弱性

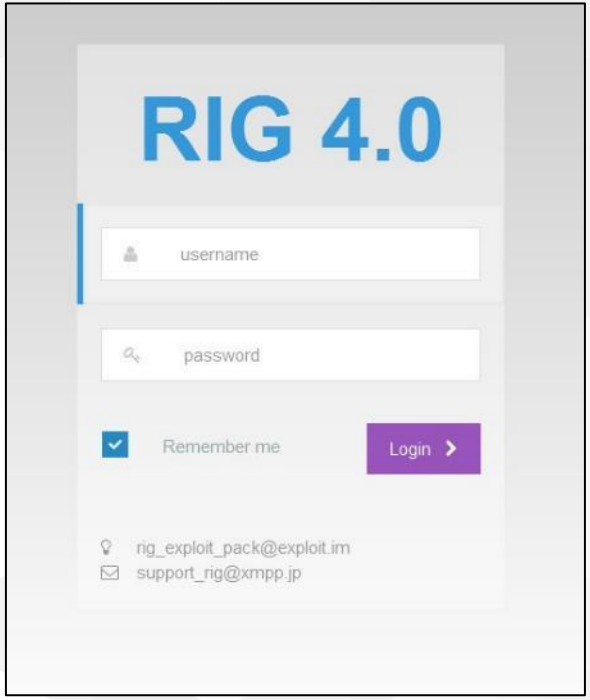
Files

Name	CRC	Size
8QrL3ThB.exe	fbb334950b935f500c934043bd03d079	379392

配布対象マルウェア

RIG EKの販売者へのコンタクト

- 連絡先の掲載場所
  - –コントロールパネルのログインページ
- コンタクト方法
  - –XMPPクライアント
- 質問事項
  - –価格帯
  - –悪用する脆弱性
  - –攻撃のため用意するもの（本命）



ログインページ

販売者からの情報収集（価格帯）

- 1週間 700ドル、1カ月 1,700ドル

[14.02.2017 18:23:58] [redacted] im very interested in rigek. how can i buy it?
[14.02.2017 18:25:36] <rig_exploit_pack@exploit.im> week-test 700, month 1700
[14.02.2017 18:27:13] [redacted] do you accept BTC?
[14.02.2017 18:32:08] <rig_exploit_pack@exploit.im> yes
[14.02.2017 18:38:14] [redacted] thank you. I want to know detailed information about rigek. Can I get trial account or reference page url?
[14.02.2017 19:53:40] <rig_exploit_pack@exploit.im> I can give you 1 day test for $100 to try

販売者からの情報収集（悪用する脆弱性）

- 回答得られず
  - public_stats.phpの提示も無し

[14.02.2017 21:30:08] [redacted] sounds good. I'm not ready for testing so I will get in touch you next week maybe. btw, could you tell me an exploit success rate and a CVE number been used?

販売者からの情報収集（用意するもの）

- RIG EKとトラフィックがあればよい
  - –他のEKと同じ役割分担

[21:51:17] [redacted] Здравствуйте!
I got a file (executable) which I want to spread. Can I do that by using Rig EK only? or shoud I buy anything in addition?
[22:30:34] *** rig_exploit_pack@exploit.im は オフライン [Прямо сейчас меня здесь нет]
[22:18:39] <rig_exploit_pack@exploit.im> just buy traffic

[22:18:45] <rig_exploit_pack@exploit.im> and rig ek only

EKを用いた攻撃の役割分担（再掲）

まとめ

- RIG EKは現在も利用されているEK
- RIG EKに関する調査方法を共有
  - 管理サーバの機能を用いたドメイン/IPアドレスの収集
  - 文字列および構造の特徴に基づいた悪用される脆弱性の特定
  - 販売者からの情報収集による背後関係の調査
- 多角的な調査により検知精度と分析品質の向上が可能

ホワイトペーパー

- 下記URLにて公開しています
  https://www.nttsecurity.com/ja-jp/Resources

NTT Security

参考文献

[1] Security Next, "エクスプロイトキット「RIG」が活発 - 国内サイト経由でランサム誘導", http://www.security-next.com/074841

[2] Security Next, "「RIG EK」による感染被害が急増 - 警察が約300の踏み台サイトに指導", http://www.security-next.com/078077

[3] Trustwave, "RIG Exploit Kit – Diving Deeper into the Infrastructure", https://www.trustwave.com/Resources/SpiderLabs-Blog/RIG-Exploit-Kit-%E2%80%93-Diving-Deeper-into-the-Infrastructure/

[4] ytif, "A repository of LIVE malwares for your own joy and pleasure", https://github.com/ytisf/theZoo/tree/master/malwares/Source/Original/ExploitKit.RIG

[5] The Register, "World's worst exploit kit weaponises white hats' proof of concept code", https://www.theregister.co.uk/2016/07/18/thanks_worlds_worst_exploit_kit_hoovers_up_white_hat_ie_exploit/

[6] The Register, "Sundown exploit kit authors champions of copy-paste hacking", https://www.theregister.co.uk/2016/09/05/sundown_exploit_kit_authors_champions_of_copypaste_hacking/

[7] VUPEN, “Advanced Exploitation of Internet Explorer 10 / Windows 8 Ov erflow (Pwn2Own 2013)”, http://www.vupen.com/blog/20130522.Advan ced_Exploitation_of_IE10_Windows8_Pwn2Own_2013.php

[8] FireEye, "CVE-2015-2419 – Internet Explorer Double-Free in Angler EK", https://www.fireeye.com/blog/threat-research/2015/08/cve-2015-2419_inte.html

[9] Theori, “PATCH ANALYSIS OF CVE-2016-0189”, http://theori.io/research/cve-2016-0189