LAC

CYBER GRID VIEW

TECHNICAL REPORT

VOL.3 I 2017


CYBER GRID JAPAN

猛威を振るう RIG Exploit Kit

執筆者　髙源 武彦、蛯原 勝徳 ＋ サイバー・グリッド研究所

1. はじめに

2017 年 2 月 2 日、一般財団法人 日本サイバー犯罪対策センター（以下、JC3）[1] が「RIG-EK 改ざんサイト無害化の取組」を発表しました。ラックは、この JC3 の活動に賛同し、2016 年 9 月末より急速に増加している RIG Exploit Kit（以下、RIG EK）による被害拡大の注意を促すため本レポートの公表に至りました。

RIG EK は、Angler EK や Neutrino EK など数あるエクスプロイトキットの一つです。エクスプロイトキットは、インターネット利用者の端末の脆弱性を悪用する攻撃ツールです。エクスプロイトキットは単体で動作しないため、攻撃者は改ざんサイトを用意しインターネット利用者を誘導します。誘導されたインターネット利用者は、ファイルを暗号化して身代金を要求する「ランサムウェア」や、ネットバンキングの不正送金を行う「バンキングマルウェア」に感染する可能性があります。

エクスプロイトキットを利用した一連の攻撃で重要なポイントは、Web サイト管理者とインターネット利用者の双方が被害者となることです。

Web サイト管理者：Web サイトが改ざんされ、
エクスプロイトキットが設置されたサーバに転送する仕組みを埋め込まれる
インターネット利用者：改ざんサイトへアクセスした際、
エクスプロイトキットが設置されたサーバへ転送されてマルウェアに感染させられる

こうした被害を減らすため、Web サイトの管理者およびインターネット利用者それぞれに向けた対策を 4 章で紹介します。加えてセキュリティ担当者に向けた攻撃の対策例などを紹介します。

本レポートは、JC3 への協力の中で行った調査をもとに、エクスプロイトキットを利用する攻撃の現状と対策について独自に分析し、まとめたものです。取りまとめには、ラックのセキュリティ監視センターJSOC (Japan Security Operation Center) と緊急対応サービスを提供するサイバー救急センター、そして研究部門であるサイバー・グリッド研究所の 3 部門が連携してあたりました。本レポートがサイバー犯罪被害の減少の一助になれば幸いです。

[1] 一般財団法人日本サイバー犯罪対策センター
https://www.jc3.or.jp/

2. RIG EK を使ったマルウェアの拡散に注意

本章では、Web サーバで動作する、脆弱性が存在するバージョンのコンテンツ管理システム（以下、CMS）および、そのプラグインやテーマを狙った攻撃の検知状況と、エクスプロイトキットを利用した攻撃の流れを解説します。特に 2017 年 1 月現在も継続して利用されている RIG EK に注目し、攻撃が増加した背景や組織的な攻撃活動（以下、攻撃キャンペーン）の存在について解説します。

2.1 Web サーバへの攻撃と RIG EK 検知状況

図 1 は、2016 年 9 月下旬から 12 月末までに JSOC で観測した Web サーバの改ざんを試みる攻撃元 IP アドレスの数（実線）と RIG EK の検知件数（破線）をグラフにしたものです。

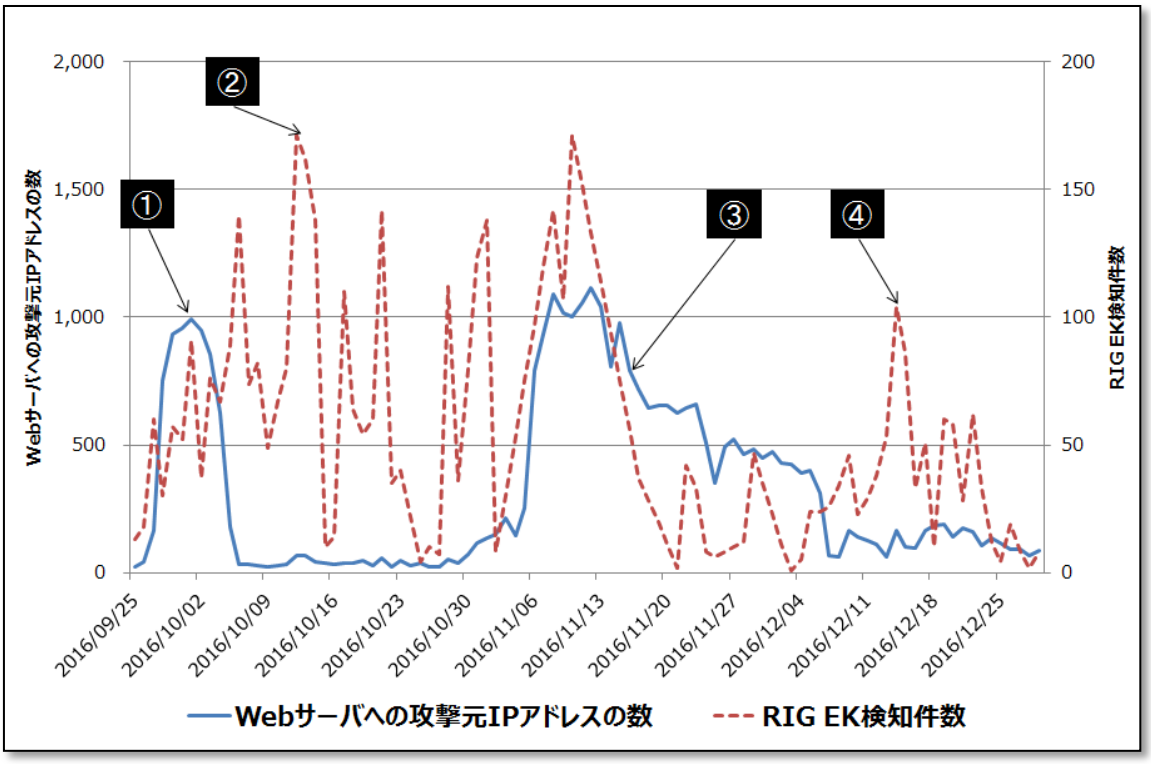

図 1 Web サーバへの攻撃と RIG EK の検知状況

Web サーバへの攻撃は、9 月下旬から 10 月上旬にかけて増加していることが確認できます（図 1 の①）。その後、Web サーバへの攻撃は減少しましたが、RIG EK の検知件数はむしろ増加しています（図 1 の②）。RIG EK が増加した理由は、改ざんサイトが放置されたことや、3 章で解説する攻撃キャンペーンの一つ「EITest」が活発な活動を行っていたことも挙げられます。

11 月中旬以降、Web サーバへの攻撃が継続しましたが、12 月上旬まで RIG EK の検知件数は減少しました（図 1 の③）。しかし 12 月中旬に「EITest」による攻撃が活発に行われ、RIG EK の検知件数が一時的に増加しました（図 1 の④）。JSOC では、「EITest」で悪用されていた改ざんサイトが、11 月中旬から

12 月上旬にかけ、改ざんの痕跡を確認できない時期がありました。しかし、12 月中旬に入ると同改ざんサイトが、「EITest」で利用されていることを確認しています。このことから攻撃者が意図的に攻撃時期や対象を制御するために、コンテンツを書き換えていた可能性が考えられます。なお、Web サーバの改ざんを試みる攻撃の主な対象は、WordPress や Joomla!など、日本国内でも多く利用される CMS およびそのプラグインやテーマです。特に WordPress 関係を狙った攻撃については日常的に多数検知しています。

表 1 に、狙われやすい WordPress のプラグインやテーマの一例を示します[2]。いずれも JSOC で攻撃の検知実績があるものです。WordPress のテーマの中には別のプラグインを内包しているものがあり、このプラグインを気付かないままインストールしてしまう場合があります。存在を認識されていないプラグインはバージョンアップされることがなく、結果として脆弱性が放置される恐れがあります。また、テーマのバージョンアップによりレイアウトが崩れてしまうという懸念などから、意図的にバージョンアップが控えられる場合もあります。このように、CMS のプラグインやテーマはバージョンアップが遅れ、脆弱性が放置される可能性が高いため、攻撃者は好んで狙っていると考えられます。

表 1 狙われやすい WordPress のプラグインとテーマ例

Cherry	Showbiz Pro
DZS ZoomSounds	Simple Ads Manager
Gravity Forms	Slider Revolution
InBoundio Marketing	Tevolution
jQuery File Upload	Ultimate Product Catalogue
MailPoet Newsletters	Uploadify
MailPress	WooCommerce
N Media Website Contact Form	WP All Import
PageLines	WP Symposium
ReFlex Gallery	WPshop eCommerce

※ アルファベット順

[2] JSOC INSIGHT vol.11「4.1 WebShell による Web サーバの不正な操作について」
https://www.lac.co.jp/lacwatch/report/20160517_000351.html

2.2　エクスプロイトキットを利用した攻撃の流れ

エクスプロイトキットを利用した攻撃の流れを図 2 に示します。

①　改ざんサイトへアクセス

改ざんサイトへアクセスするとインターネット利用者（以下、2 章、3 章のみ便宜的にユーザと記す）のブラウザや IP アドレスなどの端末情報から攻撃対象か判断されます。攻撃対象と判定されると、改ざんサイトに不審な iframe タグや script タグなどが埋め込まれます。

②　エクスプロイトキットが設置されたサーバへの転送

ユーザは改ざんサイトに埋め込まれたタグを意図せず読み込み、エクスプロイトキットが設置されたサーバへ転送されます。

③　脆弱性を悪用した攻撃

エクスプロイトキットはオペレーティングシステムやアプリケーション・ソフトウェアの脆弱性を悪用して攻撃を仕掛けます。特に、Microsoft Windows、Internet Explorer、Adobe Flash Player、Microsoft Silverlight などの脆弱性が多く悪用される傾向にあります（付録 A 参照）。

④　マルウェアのダウンロード

脆弱性を悪用した攻撃が成功すると、ユーザが意図しないままマルウェアのダウンロードが開始します。ダウンロードが完了すると、マルウェアは自動で不正プログラムを実行します。

⑤　C2 サーバ（Command & Control Server）との通信

感染した端末は C2 サーバと通信し、攻撃者からの命令を受けたり、端末の情報を渡したりします。なお、マルウェアによっては C2 サーバと通信しないものもあります。

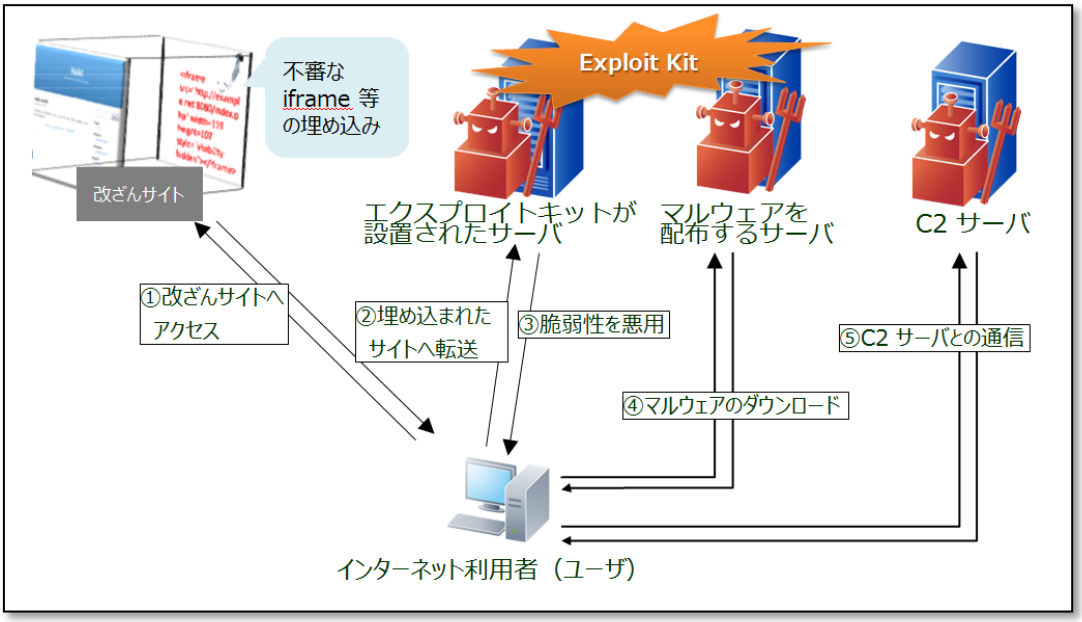

図　2　エクスプロイトキットを利用した攻撃の流れ

2.3 RIG EK による攻撃が増加した背景

RIG EK を利用する攻撃が増加した背景には、エクスプロイトキットと攻撃キャンペーンの二つの動向が関係しています。本章では、現在も RIG EK を利用している主要な三つの攻撃キャンペーンに注目し、それぞれが利用したエクスプロイトキットの 2016 年中の変遷とその要因について解説します。

図 3 に、主要な攻撃キャンペーンが利用するエクスプロイトキットの変遷を示します。いずれの攻撃キャンペーンも、ほぼ同時期に「Angler EK」、「Neutrino EK」そして「RIG EK」と変更していることが分かります。Angler EK が 2016 年 6 月以降利用されなくなった要因として、ロシアのサイバー犯罪者がロシア連邦保安庁に逮捕された事件が挙げられます[3]。この事件後、Angler EK を利用した攻撃は停滞しました。これにより、利用されるエクスプロイトキットが Neutrino EK に変わっていきました（図 3 の①）。JSOC では、各攻撃キャンペーンで利用されていた複数の改ざんサイトが、転送先を Angler EK から Neutrino EK へ切り替わっていたことを確認しています。

その後の 2016 年 9 月になると、あるセキュリティリサーチャが「Neutrino EK の作成者が提供を終了した旨のメッセージを確認した」と公表しました（図 3 の②）。同時に、このリサーチャは「実際にはパブリックな公開を終了し、一部のユーザのみが利用できるプライベートな利用形態へ移行したのではないか」とも述べています[4]。実際、Neutrino EK を利用した攻撃は減少し、同年 9 月以降は RIG EK が最も利用されるエクスプロイトキットとなりました。

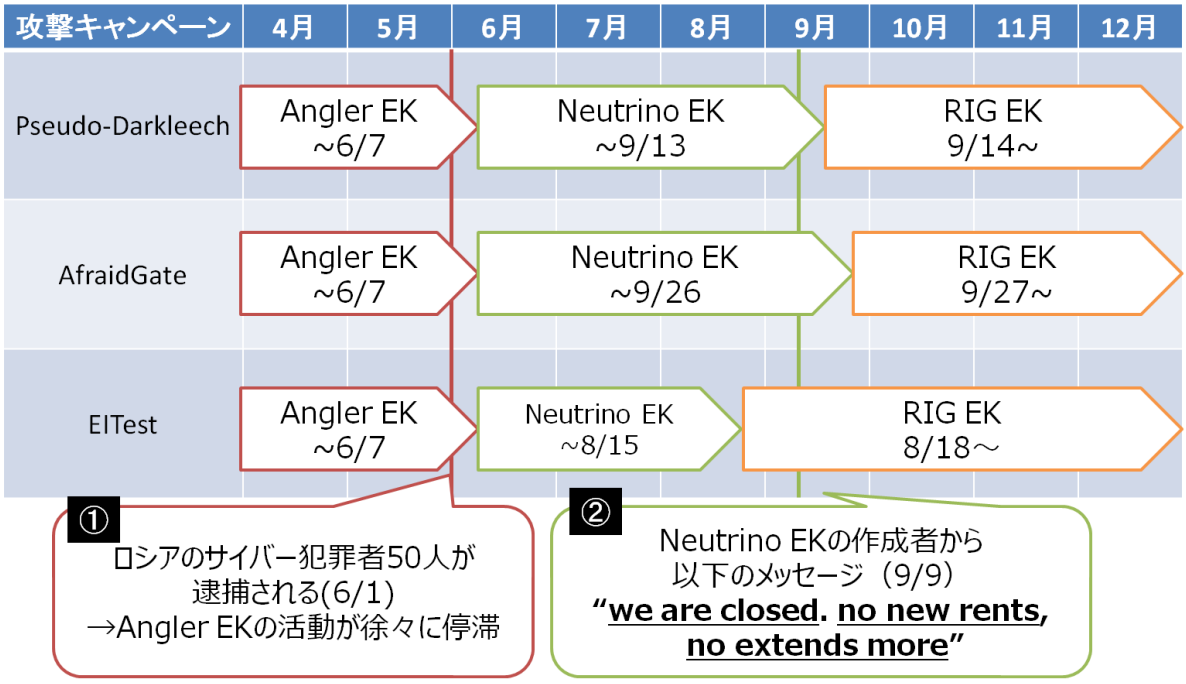

図 3 攻撃キャンペーンが利用するエクスプロイトキットの変遷（2016 年）

[3] Angler EK の活動が停滞。他のエクスプロイトキットによる新暗号化型ランサムウェア拡散を確認
http://blog.trendmicro.co.jp/archives/13538

[4] 複数のエクスプロイトキットに利用される「CERBER 4.0」
http://blog.trendmicro.co.jp/archives/13897

3. 攻撃キャンペーンの特徴

攻撃キャンペーンによって、利用するマルウェアやエクスプロイトキットへ転送する Web サイトの改ざんの痕跡が異なります。本章では RIG EK の利用が増加した要因となる三つの攻撃キャンペーン「Pseudo-Darkleech[5]」、「Afraidgate[6]」、「EITest[7]」の特徴について各節で解説します。また、現在も感染する可能性の高いマルウェアの一例をそれぞれ紹介します。

2016 年に各攻撃キャンペーンが利用した代表的なマルウェアを表 2 に示します。これは JSOC による調査および公開情報をまとめたものです。「Pseudo-Darkleech」と「Afraidgate」ではランサムウェアが多く利用される傾向にあります。一方、「EITest」はランサムウェアだけでなくバンキングマルウェア「Gootkit」、「Vawtrak」、「Ursnif」」や、ダウンローダ「Bedep」、「QuantLoader」、「SmokeBot」を利用していることを確認しています。なお、「Ursnif」についてはラック公式ブログで解説しています[8]。

表 2 攻撃キャンペーンが利用する代表的なマルウェアの変遷（2016 年）

時期	Pseudo-Darkleech	Afraidgate	EITest
4 月	Bedep 、 CryptXXX 、 TeslaCrypt	TeslaCrypt	Bedep、Gootkit、Ursnif、TeslaCrypt
5 月	Bedep、CryptXXX ClickFraud	Locky	Bedep、CryptXXX、Gootkit、Ursnif
6 月	CryptXXX	Locky	CryptXXX、CrypMIC、Gootkit、Ursnif
7 月	CryptXXX、CrypMIC	Locky	CrypMIC、Cerber、Gootkit、Ursnif
8 月	CrypMIC	Locky	Cerber、CrypMIC、Gootkit、Ursnif
9 月	CrypMIC	Locky	Cerber、Gootkit、Vawtrak、Ursnif
10 月	Cerber	Locky	Gootkit、LATENTBOT、Vawtrak、Ursnif
11 月	Cerber	Locky	LATENTBOT、QuantLoader、SmokeBot
12 月	Cerber	Locky	Gootkit、QuantLoader、SmokeBot

※ 赤字：ランサムウェア ※ 黒字：その他

[5] Campaign Evolution: pseudo-Darkleech in 2016
http://researchcenter.paloaltonetworks.com/2016/12/unit42-campaign-evolution-pseudo-darkleech-2016/

[6] Rig Exploit Kit from the Afraidgate Campaign
https://isc.sans.edu/forums/diary/Rig+Exploit+Kit+from+the+Afraidgate+Campaign/21531/

[7] EITest 攻撃の進化:Angler EK から Neutrino そして Rig へ
https://www.paloaltonetworks.jp/company/in-the-news/2016/161004-unit42-eitest-campaign-evolution-angler-ek-neutrino-rig.html

[8] Ursnif（別名：Gozi 他）が 2016 年 3 月以降猛威を振るっています。
https://www.lac.co.jp/lacwatch/people/20160615_000362.html

3.1 Pseudo-Darkleech

「Pseudo-Darkleech」が利用する改ざんサイトへアクセスすると、図 4 のようなランダムな文字列が表示されます。この時の Web サイトのソースコードには、図 4 に示された文字列が、図 5 の 6 行目にある文字列と一致していることが確認できます。図 4 がユーザの画面上に表示された裏では、図 5 の 3 行目にある iframe タグを読み込んでいます。この iframe タグにより、ユーザは本人の意思とかかわりなくエクスプロイトキットが設置されたサーバへ転送されます。

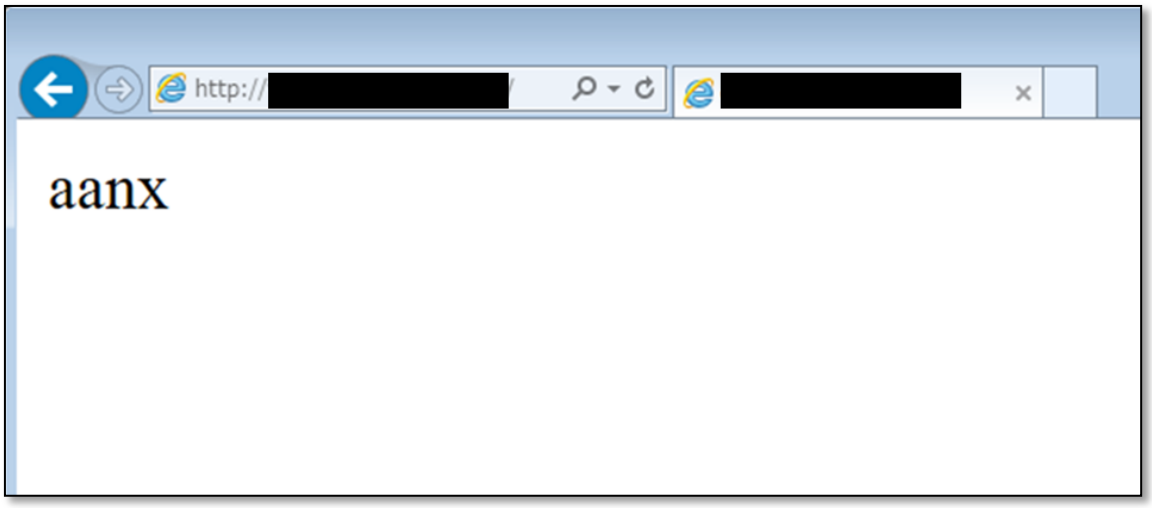

図 4 改ざんサイトへアクセスした際のブラウザ画面の一例（Pseudo-Darkleech）

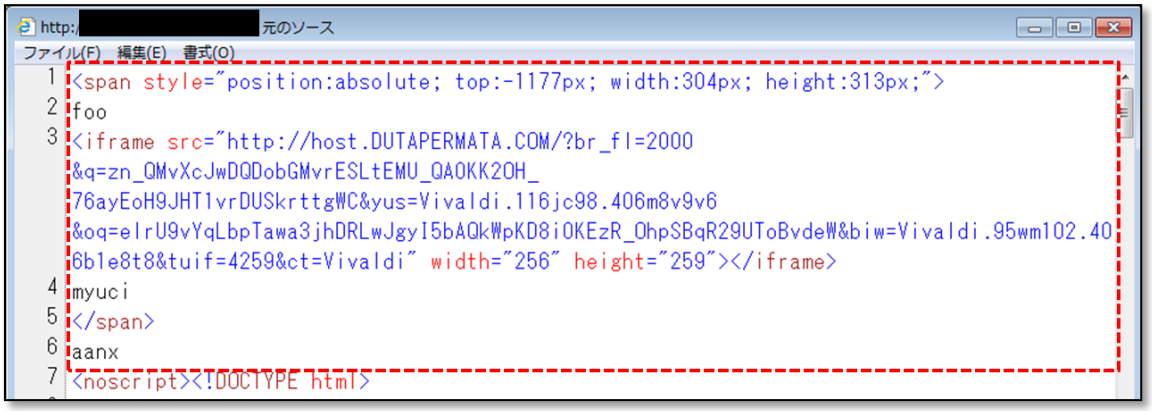

図 5「Pseudo-Darkleech」の改ざんの痕跡（2017 年 1 月）

「Pseudo-Darkleech」では、検索エンジン最適化を悪用し、ユーザが「Yahoo!」や「Google」などの検索エンジンでブランド商品や業務用器具などを調べた際に、改ざんサイトを検索結果の上位に表示します（図 6 の(a)）。これにより日本のショッピングサイトを装った結果を表示させ、ユーザをそのサイトに誘います。JSOC では、ユーザが実際にアクセスした際に存在しないページが表示され（図 6 の(b)）、エクスプロイトキットへ転送されるケースを確認しています。

(a)検索した結果　　(b)アクセスした結果

図 6　検索エンジン最適化を悪用した誘導手法

「Pseudo-Darkleech」ではランサムウェアを継続して利用しています。JSOC では、2016 年 10 月以降ランサムウェア「Cerber」に感染することを確認しています。「Cerber」はユーザの端末にあるデータを暗号化し、図 7 の(a)のようにデスクトップを書き換え、金銭を要求する画面を言語環境に合わせて表示します（図 7 の(b)）。さらに、感染後は 6892 ポート宛の UDP 通信が大量に発生するという特徴があります（図 8）。

(a)デスクトップ背景　　(b)説明書

図 7　ランサムウェア「Cerber」感染後の画面

No.	Time	Destination	Protocol	Length	Info
728	2017-01-17 04:48:52…	90.2.1.3	UDP	67	51489 → 6892 Len=25
729	2017-01-17 04:48:52…	90.2.1.4	UDP	67	51489 → 6892 Len=25
730	2017-01-17 04:48:52…	90.2.1.5	UDP	67	51489 → 6892 Len=25
731	2017-01-17 04:48:52…	90.2.1.6	UDP	67	51489 → 6892 Len=25
732	2017-01-17 04:48:52…	90.2.1.7	UDP	67	51489 → 6892 Len=25
733	2017-01-17 04:48:52…	90.2.1.8	UDP	67	51489 → 6892 Len=25
734	2017-01-17 04:48:52…	90.2.1.9	UDP	67	51489 → 6892 Len=25
735	2017-01-17 04:48:52…	90.2.1.10	UDP	67	51489 → 6892 Len=25
736	2017-01-17 04:48:52…	90.2.1.11	UDP	67	51489 → 6892 Len=25
737	2017-01-17 04:48:52…	90.2.1.12	UDP	67	51489 → 6892 Len=25
738	2017-01-17 04:48:52…	90.2.1.13	UDP	67	51489 → 6892 Len=25
739	2017-01-17 04:48:52…	90.2.1.14	UDP	67	51489 → 6892 Len=25
740	2017-01-17 04:48:52…	90.2.1.15	UDP	67	51489 → 6892 Len=25
741	2017-01-17 04:48:52…	90.2.1.16	UDP	67	51489 → 6892 Len=25
742	2017-01-17 04:48:52…	90.2.1.17	UDP	67	51489 → 6892 Len=25
743	2017-01-17 04:48:52…	90.2.1.18	UDP	67	51489 → 6892 Len=25
744	2017-01-17 04:48:52…	90.2.1.19	UDP	67	51489 → 6892 Len=25

図 8 ランサムウェア「Cerber」感染後の UDP 通信

ランサムウェアの対策は、定期的にバックアップを取得することです。それにより、万が一ランサムウェアの被害に遭ったとしても、損失したデータを復旧することができます。

なお、ランサムウェアの一般的な対策については、4.4 節で解説します。

3.2 Afraidgate

「Afraidgate」が利用する改ざんサイトへアクセスすると、先に述べた「Pseudo-Darkleech」とは異なり、見かけ上は正規のページが表示されます。しかし、図 9 に見られるように、外部ホストからエクスプロイトキットが設置されたサーバへ転送する Javascript を読み込みます。

なお、このホスト「misterin[dot]pkitup[dot]com」は、Afraid.org で登録されたものです（図 10）。

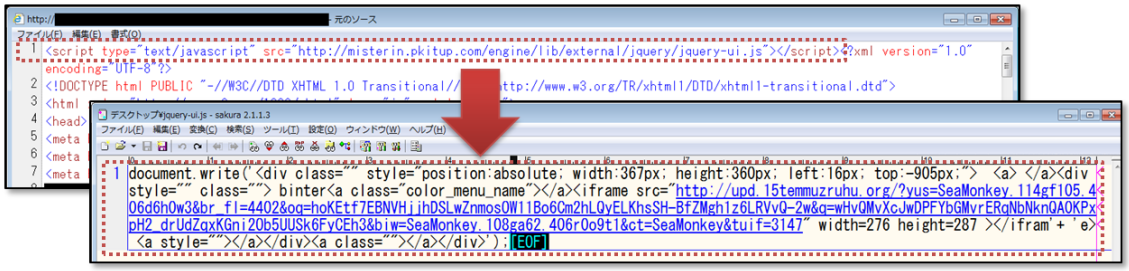

図 9 「Afraidgate」の改ざんの痕跡（2017 年 1 月）

Afraid.org は、ダイナミック DNS サービスを提供しています。図 10 のように、所有するドメインの「Status」を「public」として登録すると、自由にサブドメインを追加できてしまい、「Afraidgate」をはじめとした攻撃に悪用されることになります。Afraid.org などのダイナミック DNS サービスを利用する場合は、設定を十分に確認し、サブドメインが勝手に登録されないよう、注意が必要です。

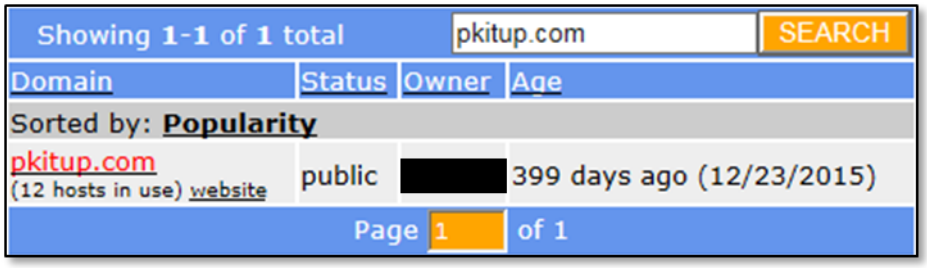

図 10　Afraid.org で登録されたドメイン(pkitup[dot]com)

「Afraidgate」では 2016 年 5 月以降、継続してランサムウェア「Locky」を利用しています。

「Locky」に感染したユーザの端末は、オペレーティングシステムの言語等の情報を C2 サーバへ送信するとともに端末のデータを暗号化します。その後デスクトップを書き換え、金銭を要求する画面を言語環境に合わせて表示します(図 11)。

図 11　ランサムウェア「Locky」感染後の金銭要求画面

表 3　ランサムウェア「Locky」感染時期による POST 通信の違い

時期	POST 通信の URL
2016/8/23～	/data/info.php
2016/9/27～	/apache_handler.php
2016/10/25～	/linuxsucks.php
2016/11/3～	/message.php
2016/11/21～	/information.cgi
2016/12/5～	/checkupdate

「Locky」に感染した時期により、表 3 のように感染時に発生する POST 通信の URL が異なります。C2 サーバの IP アドレスやドメインは毎日のように変わりますが、POST 通信の URL は一定期間利用されるため、表を参考に Proxy ログ等で該当する通信の有無を確認することを推奨します。「Locky」感染時に発生する POST 通信の例を図 12 に示します。

図 12　ランサムウェア「Locky」感染時に発生する POST 通信

3.3 EITest

「EITest」が利用する改ざんサイトへアクセスすると、「Afraidgate」と同様に見かけ上は正規のページが表示されます。ただし、「Afraidgate」と異なり、エクスプロイトキットが設置されたサーバへ直接転送するscriptタグが改ざんサイトに埋め込まれています（図 13）。

図 13 「EITest」の改ざんの痕跡（2016 年 12 月）

国外では「EITest」による攻撃が行われているにもかかわらず、JSOC で調査した際は、国内では改ざんの痕跡およびエクスプロイトキットへの転送を確認できない時期がありました。そのため、攻撃者が攻撃の対象を制御していると考え、オープンプロキシの ON/OFF を切り替えて改ざんサイトへアクセスし、異なる国の IP アドレスを用いて応答ページに含まれる改ざんの痕跡を調査しました。

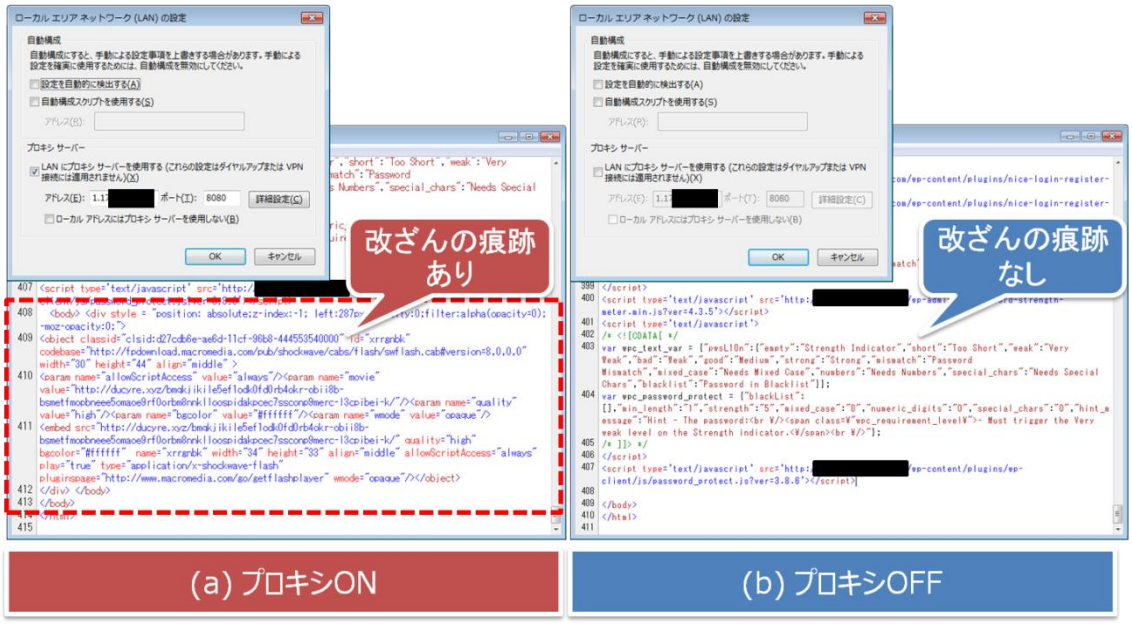

図 14 国外の IP アドレスが割り当てられたプロキシ ON/OFF 時の応答ページの違い

オープンプロキシを利用してアクセスした際は、図 14(a)中の破線枠内にエクスプロイトキットへ転送する改ざんの痕跡が確認できました。一方、オープンプロキシを利用せずアクセスした際は、図 14(b)で示すとおり、同様の改ざん痕跡は確認できませんでした。この国外の IP アドレスが割り当てられたオープンプロキシを利用した調査から、攻撃者がアクセス元の IP アドレス、国など端末情報を収集し、意図的に標的を制御していた可能性が考えられます。このように、一見 Web サイトの改ざん被害はないと思われる場合でも、異なる端末情報でアクセスすると改ざんが確認できることがあります。

「EITest」では、2016 年 11 月上旬以降「QuantLoader」というダウンローダを利用しています。「QuantLoader」は、図 15 のように外部ホストから実行ファイルをダウンロードし、「LATENTBOT[9, 10]」というバックドアに感染させます。なお、「EITest」はランサムウェアやバンキングマルウェアなど、さまざまなマルウェアを利用しているため注意が必要です。

```
GET /quant/index.php?id=75547828&c=1&mk=ca1a0f HTTP/1.1
Accept: */*
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64;
Trident/7.0; 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; GWX:QUALIFIED)
Host: [redacted]
Connection: Keep-Alive

HTTP/1.1 200 OK
Date: Wed, 09 Nov 2016 23:47:41 GMT
Server: Apache/2.2.15 (CentOS)
X-Powered-By: PHP/5.6.28RC1
Content-Length: 39
Connection: close
Content-Type: text/html; charset=UTF-8

exe=http:/[redacted]/lich0911.exe;
```

図 15 ダウンローダ「QuantLoader」感染時の通信

[9] LATENTBOT: Trace Me If You Can
https://www.fireeye.com/blog/threat-research/2015/12/latentbot_trace_me.html
[10] FireEye、企業に侵入する高難読化バックドア「LATENTBOT」を発見
https://the01.jp/p0001663/

4. 対策

本章では、Web サイト管理者およびインターネット利用者に向けて、エクスプロイトキットの被害を緩和するための対策例を紹介します。加えて、セキュリティ担当者向けに攻撃の対策例と被害状況の確認方法を紹介します。

4.1 Web サイト管理者に推奨する対策例

- **オペレーティングシステムやアプリケーション・ソフトウェアを最新の状態に保つ**

攻撃者はオペレーティングシステムや CMS の脆弱性を悪用して攻撃を実施します。自身の管理する Web サイトが攻撃者に悪用されないために、利用環境への影響を確認した上で、常に最新版を利用することが重要です[11]。

- **複雑なパスワードを活用する**

改ざんは、正規のユーザアカウントに不正ログインされて行われることがあります。特に、初期設定のままのパスワードや推測されやすい単純なパスワード、短いパスワードの使用は、総当り攻撃やリスト型の攻撃などに対して弱点となります。推測されにくく複雑なパスワードを作るために、8 文字以上かつ大小英字、数字、記号など異なる文字種を組み合わせることが一般的に推奨されています[12]。

- **セキュリティ製品およびセキュリティサービスを導入する**

IDS/IPS および WAF 等のセキュリティ製品や、マネージド・セキュリティ・サービス（以下、MSS）およびセキュリティ診断等のセキュリティサービスの導入は、攻撃や脆弱性の早期発見につながります。MSS はセキュリティ製品を導入した後の運用・監視を行い、外部からの攻撃や内部からの情報漏えい等に対して早期対応するためのサービスです。また、セキュリティ診断は Web サイトやサーバに脆弱性が存在しないかを調査し、攻撃者に悪用されるリスクを減らすためのサービスです。

- **適切な設定で運用を行う**

Web サーバの公開ディレクトリに対するファイル作成を制限することや、実行プログラムへのアクセスを制限することで、攻撃による影響の緩和が見込めます。また万が一、不正なファイルがアップロードされた場合に備え、ウイルス対策ソフトによる定期的なファイルスキャンを実施するとともに、ファイルの改ざん検知の仕組みを取り入れると効果的です。不正なファイルのアップロードを防ぐための対策例として推奨する事項を次に示します。

□Web 公開ディレクトリに対するファイル作成権限の制限
□リクエストデータ長の制限
□PHP ファイルのようなサーバサイドで実行するプログラムへの直接アクセスの制限

[11] CMS を用いたウェブサイトにおける 情報セキュリティ対策のポイント
https://www.ipa.go.jp/files/000054743.pdf
[12] STOP!!パスワード使い回し!!キャンペーン 2016
https://www.jpcert.or.jp/pr/2016/pr160003_detail.html

- **ログを保管する期間を見直す**

Web サイトの改ざん被害にいち早く気づき、事後対応を迅速かつ効果的に進めるためには、ログの取得と保管が大変重要です。しかし、ログを取得していたとしても保管期間がわずか 1 カ月程度と短いと、改ざん原因の調査が難航する恐れがあります。ログの保管期間を延長、外部媒体へのバックアップするなど、社内のセキュリティレベルに合わせたログの見直しを推奨します[13]。

なお、セキュリティベンダーや外部団体より改ざんの指摘を受けた場合は、被害の拡大を防ぐため早急な対応が必要です。具体的には、Web サイトを一旦公開停止した上で原因究明と対処を並行して進めます。万が一の改ざん被害でお困りのことがありましたら、ラックのサイバー救急センター[14]までご相談ください。

4.2 インターネット利用者に推奨する対策例

- **ウイルス対策ソフトを最新の定義ファイルに更新する および 定期的なスキャンを実施する**

ウイルス対策ソフトは、導入後も最新の定義ファイルに更新し続ける必要があります。近年のウイルス対策ソフトは、ヒューリスティックや振る舞い検知、レピュテーション機能等があり、未知の攻撃を防ぐこともあります。

- **オペレーティングシステムやアプリケーション・ソフトウェアを最新の状態に保つ**

エクスプロイトキットは、オペレーティングシステムやアプリケーション・ソフトウェアの脆弱性を悪用し、攻撃を仕掛けます。そのため、ウイルス対策ソフトを導入している場合でも、セキュリティホールをなくすためにオペレーティングシステムやアプリケーション・ソフトウェアを最新の状態で維持することが重要です。過去には、アップデートパッチの公開からわずか 3 日でエクスプロイトキットに攻撃コードが組み込まれた例もあるため、迅速なパッチ適用が重要です。

- **ブラウザを使い分ける**

RIG EK に対しては、ブラウザの使い分けが簡易的な対策となります。RIG EK では、インターネット利用者の User-Agent を確認し、Internet Explorer を使用していた場合に攻撃を行うことが確認されています[15]。業務都合上、Internet Explorer や関連するプラグイン（Adobe Flash Player や Silverlight 等）をアップデートできない場合は、Internet Explorerの利用を社内システムのみにとどめ、インターネットへのアクセスには他のブラウザを利用するなど、適切に使い分けを実施することで RIG EK に転送されるリスクを軽減することができます。

13「企業における情報システムのログ管理に関する実態調査」報告書について
https://www.ipa.go.jp/security/fy28/reports/log_kanri/

14 緊急対応サービス「サイバー119」
https://www.lac.co.jp/service/consulting/cyber119.html

15 pseudoDarkleech Leads to Rig-V EK at 194.87.232.99 and Drops Cerber. New Fingerprinting Technique / Gate?
https://malwarebreakdown.com/2016/12/05/pseudodarkleech-leads-to-rig-v-ek-at-194-87-232-99-and-drops-cerber-new-fingerprinting-techniquegate/

4.3　セキュリティ担当者に推奨する対策例

- **ネットワーク機器等による対策と検知方法**

インターネット利用者がRIG EKへ転送される際には、特徴的な文字列がURLに含まれます。表４の通り、RIG EK が使用する URL は大きく３パターンに分類されます。表中の赤文字は RIG EK のパターン分類に使われる「固定文字列」で、この文字列の有無が RIG EK へ転送されているかを確認する重要な手がかりとなります。「固定文字列」はすべてのパターンで観測でき、パターン１では「QMvXcJ」、パターン２では「WrwE0q」、パターン３では「fPrfJxzFGMSUb-nJDa9」が使われています。そのため、対策としてはProxyログ等で「固定文字列」を含む通信の有無を確認した上で、該当する通信があればURLフィルタリングソフトで遮断することを推奨します。

表 4 RIG EK が使用する URL

RIG EK	観測時期	URL に含まれる文字列例
パターン１	2016/12/30～	/?ct=Amaya&tuif=3990&oq=F86[略]8jg&br_fl=4836&q=znn**QMvXcJ**wDQ[略]ly&yus=Amaya.75[略]0b0&biw=Amaya.98[略]4r2
	2016/10/24～	/?sourceid=edge&aqs=edge.90[略]8z0&q=wXf**QMvXcJ**wDQ[略]16B&oq=2aC[略]Tp1&es_sm=151&ie=Windows-1252
パターン２	2016/11/9～	/?sourceid=edge&es_sm=119&q=LbX**WrwE0q**0Y[略]pII&ie=UTF-16&oq=Dgt[略]Ucp&aqs=edge.121c68.406i0q6
パターン３	2015/5/7～	/?w3aKdrifKx7JCII=l3SK**fPrfJxzFGMSUb-nJDa9**BMEX[略]nOBKqE

- **RIG EK による被害状況の確認方法**

次に、RIG EK の一連の攻撃がどの段階まで進んだかを確認する方法を解説します。その際に重要な要素は「Content-Type」ヘッダです。図 16 に RIG EK の攻撃通信の遷移を示します。

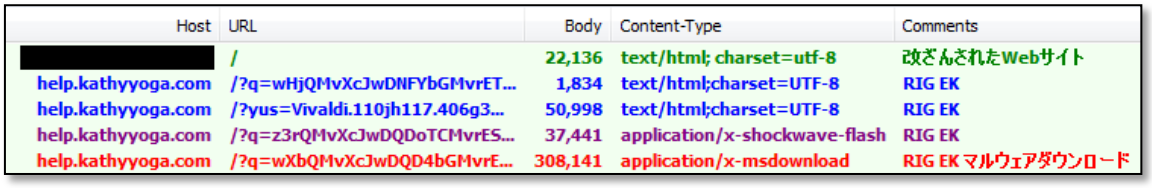

図 16 RIG EK の攻撃通信遷移

「Content-Type」が「application/x-msdownload」となっていた場合は、マルウェアをダウンロードする通信です。このような通信が確認された場合は端末がマルウェアに感染している可能性が高いため、その後の通信を調査する必要があります。

一方、「Content-Type」が「application/x-shockwave-flash」や「text/html」の通信で終了していた場合は、RIG EK の攻撃が失敗に終わったことを示しており、マルウェアのダウンロードには至っていないと言えます。このように、「Content-Type」を見ることで、RIG EK による一連の攻撃の進行状況を確認することが可

能です。RIG EK による攻撃被害状況の確認やその他の脅威に備えるためにも、URL 文字列や「Content-Type」ヘッダを確認できるようなログの取得・保存を推奨します。

ただし、ここまで述べた特徴は、本レポートを執筆中の 2017 年 1 月現在、継続している RIG EK のものであることに注意が必要です。今後登場する別バージョンの RIG EK および RIG EK 以外のエクスプロイトキットでは、ここで紹介したものとは異なる URL 文字列や「Content-Type」が使われる可能性がありますので、それぞれに応じた対策を講じる必要があります。

4.4 ランサムウェアの対策例

ランサムウェアの感染事例が国内外で相次いでいます。国外では、身代金を支払うことで復号鍵を入手し、ファイルを復号した事例も報告されていますが、金銭を支払ったとしても復号できる保障はありません。ランサムウェアの感染被害に遭わないため、また予防するためには、以下の対策を実施することが重要です[16]。

□ オペレーティングシステムとアプリケーション・ソフトウェアを最新の状態にアップデートする
□ ウイルス対策ソフトを最新の定義ファイルに更新する
□ 不審なメールの添付ファイルを開かない、不審なメール本文にある URL へアクセスしない
□ 手口や被害事例について、常に最新の情報をセキュリティ情報サイトやニュースサイトから入手する
□ 外部の不正サイトへのアクセスをブロックする
□ 重要なデータは物理的に切り離された外部ストレージに定期的にバックアップする

[16] IPA テクニカルウォッチ「ランサムウェアの脅威と対策」
http://www.ipa.go.jp/security/technicalwatch/20170123.html

5. おわりに

本レポートでは、RIG EK を利用する攻撃について解説しました。その上で、攻撃被害状況の確認方法と被害緩和のための対策例を紹介しました。RIG EK の被害を減らすには、Web サイト管理者とインターネット利用者のどちらか一方ではなく、双方で対策を講じることが不可欠です。中でも、「オペレーティングシステムやアプリケーション・ソフトウェアを最新の状態に保つことは、被害を減少させる重要な対策の一つです。

2016 年 11 月中旬以降、RIG EK への検知件数が減少しています。一方で、JSOC では 2017 年 1 月現在、Sundown EK を利用する攻撃事例を確認しています。加えて、攻撃キャンペーン「EITest」が、RIG EK 以外にも、Sundown EK やエクスプロイトキットを利用せずにマルウェア感染させているという情報もあります[17, 18]。過去には、「EITest」が利用するエクスプロイトキットを変えた後に、他の攻撃キャンペーンも利用するエクスプロイトキットを変更したことがあり、注意が必要です。

攻撃者の利用するエクスプロイトキットは変化していきますが、改ざんサイトは継続して利用される可能性があります。被害の拡大および自社の Web サイトが攻撃に悪用されないために、セキュリティベンダーや外部団体から通知があった場合には、迅速に対応することが期待されます。

サイバー攻撃は日々変化し、より巧妙になっています。新しい攻撃手法や脆弱性に対処するには日々、情報収集に努め、攻撃者などの動向を把握し、状況に応じて対策を施す必要があります。対策を実施するにあたっては、国内の下記サイトも参考になります。

- JC3(一般財団法人 日本サイバー犯罪対策センター)
  https://www.jc3.or.jp/
- JVN: Japan Vulnerability Notes
  https://jvn.jp/
- JPCERT/CC(一般社団法人 JPCERT コーディネーションセンター)
  https://www.jpcert.or.jp/
- IPA(独立行政法人 情報処理推進機構)
  https://www.ipa.go.jp/

ラックは安心・安全な情報社会に寄与するため、今後も継続的にエクスプロイトキットや攻撃キャンペーンの動向について調査し、広く情報を提供していきたいと考えています。

---

[17] EITest Nabbing Chrome Users with a “Chrome Font” Social Engineering Scheme
https://www.proofpoint.com/us/threat-insight/post/EITest-Nabbing-Chrome-Users-Chrome-Font-Social-Engineering-Scheme

[18] Exposing EITest campaign
https://blog.brillantit.com/exposing-eitest-campaign/

A. 付録

表 A は、各エクスプロイトキットが悪用するオペレーティングシステムやアプリケーション・ソフトウェアの脆弱性を 2017 年 1 月までの公開情報からまとめたものです。

表 A 各エクスプロイトキットが悪用する脆弱性

対象脆弱性アプリケーション		CVE 番号	Angler EK	RIG EK	Neutrino EK
Adobe Flash Player	21.0.0.241 以前	CVE-2016-4117	●	-	●
	20.0.0.306 以前	CVE-2016-1019	-	●	●
	20.0.0.306 以前	CVE-2016-1001	●	-	-
	20.0.0.235 以前	CVE-2015-8651	●	●	●
	19.0.0.245 以前	CVE-2015-8446	●	-	-
	19.0.0.207 以前	CVE-2015-7645	●	-	●
	18.0.0.209 以前	CVE-2015-5560	●	-	-
	18.0.0.203 以前	CVE-2015-5122	●	●	●
	18.0.0.194 以前	CVE-2015-5119	●	●	●
	18.0.0.161 以前	CVE-2015-3113	●	●	●
	17.0.0.188 以前	CVE-2015-3105 CVE-2015-3104	●	-	-
	17.0.0.169 以前	CVE-2015-3090	●	●	●
	17.0.0.134 以前	CVE-2015-0359	●	●	●
	16.0.0.305 以前	CVE-2015-0336	●	-	●
	16.0.0.296 以前	CVE-2015-0313	●	-	●
	16.0.0.287 以前	CVE-2015-0311	●	●	●
	16.0.0.257 以前	CVE-2015-0310	●	-	-
	15.0.0.189 以前	CVE-2014-8440	●	-	-
	13.0.0.252 以前	CVE-2014-8439	●	-	-
	15.0.0.167 以前	CVE-2014-0569	●	●	●
	13.0.0.182 以前	CVE-2014-0515 CVE-2013-0634	-	-	●
Microsoft Windows	MS14-064 (3006226)	CVE-2014-6332	-	-	●
	MS14-052 (2977629)	CVE-2013-7331	●	-	-
Silverlight	MS16-006 (3126036) 5.1.41212.0 以前	CVE-2016-0034	●	●	-
	MS15-044 (3057110) 5.1.40416.00 以前	CVE-2015-1671	●	-	-
	MS13-087 (2890788) 5.1.20913.0 以前	CVE-2013-3896	●	●	-
	MS13-022 (2814124) 5.1.20215.0 以前	CVE-2013-0074	●	●	-
Internet Explorer	MS16-051 (3155533)	CVE-2016-0189	-	●	●
	MS15-065 (3076321)	CVE-2015-2419	●	●	●
	MS14-064 (3011443)	CVE-2014-6332	-	-	●
	MS14-056 (2987107)	CVE-2014-4130	●	-	-
	MS14-012 (2934088)	CVE-2014-0322	●	●	-
	MS14-052 (2977629)	CVE-2013-7331	●	●	-
	MS13-037 (2829530)	CVE-2013-2551	●	●	●

「●」：公開情報あり「-」：公開情報なし


CYBER GRID JAPAN

LAC Co., Ltd.
CYBER GRID Laboratory