平成 29 年２月２日

各位

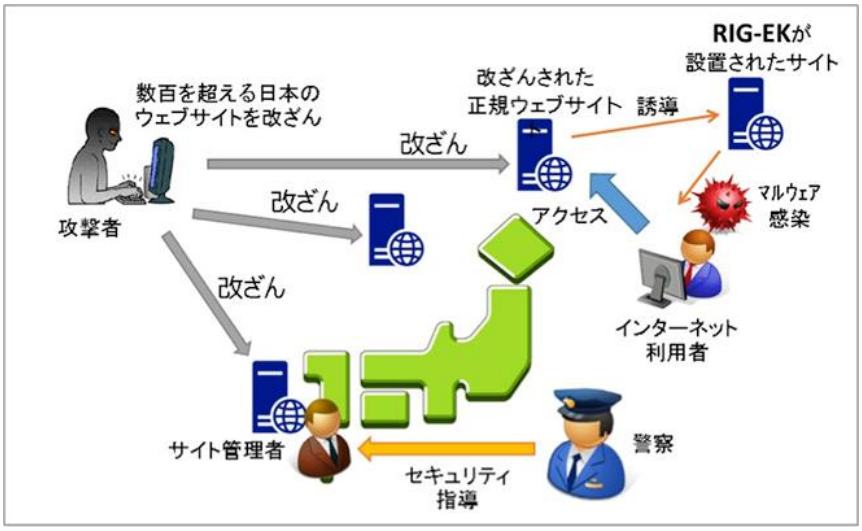
会 社 名　株　式　会　社　ラ　ッ　ク
代表者名　代表取締役社長　髙　梨　輝　彦
（JASDAQ・コード番号：３８５７）
問合せ先　ＩＲ広報室長　岩　﨑　　勝
電　　話　０３－６７５７－０１０７

ラック、JC3 が取り組む改ざんサイトの無害化活動に参加
～攻撃ツール RIG-EK により拡大する改ざんサイトの無害化に技術協力～

株式会社ラック（本社：東京都千代田区、代表取締役社長：髙梨 輝彦、以下ラック）は、一般財団法人 日本サイバー犯罪対策センター（以下JC3）と全国の都道府県警察が進める、攻撃ツール「RIG Exploit Kit（以下RIG-EK：リグ イーケイ）」により改ざんされたサイトの無害化活動に技術協力し、サイバー攻撃の全容解明とインターネット利用者保護に取り組みます。

最近は日本においても、多くのインターネット利用者からの金銭窃取を目的とした、ランサムウェアと呼ばれる身代金要求型ウイルスやインターネットバンキングの不正送金ウイルスなどによる被害が拡大しています。その一部は、攻撃ツール「RIG-EK」により行われていると推測しています。攻撃者は正規サイトのコンテンツを改ざんし、サイトの閲覧者をRIG-EKが設置されたサイトへ誘導し、感染させていることが確認されました。このような攻撃は、「水飲み場型攻撃」ともいわれ、ラックでは2013年10月に注意喚起情報を公開しています。

そこでJC3は、改ざんされた正規サイトの情報を関係する都道府県警察に提供し、地域ごとで適切な対応を行っていただくことにより日本全国に広がっている改ざんされたサイトの管理者へセキュリティ対策の指導を行うことで、改ざんサイトを無害化する活動を実施します。



ラックは、2014年11月よりJC3に参画し、サイバー空間の脅威に関する情報の提供と、分析・対処手法の検討などの技術協力を行ってきました。ラックが運営するセキュリティ監視センターであるJSOCで検知したRIG-EKに関する膨大な情報の提供および、JC3内で組織される不正送金事犯情報分析プロジェクトおよび脅威情報活用WGへ技術者を派遣することなどにより、拡大するRIG-EKの脅威に対しての取り組みを進めています。

サイト管理者、一般組織、インターネット利用者における注意事項について

RIG-EK による脅威に関して、インターネット利用者はもちろん、サイト管理者側も深刻な現状を理解のうえ、次の対応をお願いします。

サイト管理者へ推奨する対策例

- 正規のサイト管理者になりすまして不正ログインを行い改ざんされる事例があるため、初期設定のパスワードや推測されやすい単純なパスワード、短いパスワードではなく、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て作成してください。
- また、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が行われることもあるため、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、ご利用環境に重篤な脆弱性が存在していないかを確認のうえ、常に最新版を利用するなど適切な対策をお願いします。
- 対策には、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、攻撃の発見や遮断、脆弱性の早期発見につながります。外部専門家の活用も是非検討ください。
- 攻撃者が RIG-EK や不正なファイルアップロードし、サイトを悪用するには、ファイルの作成やそのファイルに外部からアクセスできなくてはなりません。そのため、ファイル作成権限、サイトでの実行プログラムの制限や不正プログラムへの連絡を断つためにリクエストデータ長の制限などの対策も有効です。
- 万一被害に逢った場合、被害状況や影響範囲の調査など、事後対応を効果的に行うためにはログの取得と保管が必要です。サイトの重要性を考慮してログ取得内容と保管期間を見直してください。

サイバー攻撃により感染被害を受ける一般組織へ推奨する対策例

- RIG EK へ転送される際には、特徴的な文字列を URL に含まれます。プロキシサーバーのログ等で「固定文字列」を含む通信有無の確認や URL フィルタリングソフトにて該当する通信を遮断することを推奨します。確認方法は、CYBER GRID VIEW Vol.３をご覧ください。
- RIG EK の一連の攻撃がどの段階まで進んだかを確認し、被害の状況を把握してください。確認方法は、CYBER GRID VIEW Vol.３をご覧ください。

サイバー攻撃により感染被害を受けるインターネット利用者へ推奨する対策例

- ウイルス対策ソフトを導入し、新しい不正プログラムを検出するための定義ファイル（パターンファイル）を最新のものに更新してください。
- Windows 等の基本ソフト（OS）の自動更新機能等を利用し、常に最新の状態を維持してください。また、その他ウェブ閲覧と関連するウェブブラウザ等のソフトウェアについても、各セキュリティパッチを適用して最新の状態を維持してください（脆弱性を解消）。
- 現在の RIG-EK は、インターネット利用者が Internet Explorer を使用している場合に、攻撃を行うことが確認されています。一時的な対策としては、Internet Explorer 以外のブラウザの利用を検討してください。
- ランサムウェアに対抗するために、定期的に重要なデータを物理的に切り離されたストレージにバックアップしてください。

ここに取り上げた RIG-EK に関する技術的な説明については、CYBER GRID VIEW Vol.３をお読みください。

ラックは、JC3 および都道府県警察の取り組みを支援することで、今後も安心安全なインターネット活用に寄与してまいります。

▼参考情報

- 攻撃ツール RIG-EK とは
  RIG-EK に含まれる EK は Exploit Kit の略で、エクスプロイトキットと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する攻撃ツールです。RIG-EK は、インターネット利用者に身代金要求ウイルスや不正送金ウイルスを配布するため、正規の Web サイトを改ざんしウイルス配布サーバーへ誘導するために用いられます。
  RIG-EK に関する詳細は、CYBER GRID VIEW Vol.３をお読みください。
- JC3 の注意情報
  RIG-EK 改ざんサイト無害化の取組

以上

【 株式会社ラックについて 】　(https://www.lac.co.jp/)
ラックは、1986年にシステム開発事業で創業、多くの実績を誇る「金融系の基盤システム開発」「マーケティング・オートメーション支援」「ビッグデータ・アナリティクス」を始め、社会の基盤システムの開発を行っています。1995年にはいち早く情報セキュリティ事業を開始し、現在ではサイバーセキュリティ分野のリーディングカンパニーとして、官公庁・企業・団体等のお客様に業界屈指のセキュリティ技術を駆使した、先端のITトータルソリューションサービスを提供しています。2016年には、米フロスト＆サリバンより、「セキュリティ監視」「脆弱性診断」「セキュリティ事故対応」「セキュリティコンサルティング」などが高く評価され、昨年に続き２年連続で「2016 ジャパン マネージドセキュリティサービス プロバイダーオブザイヤー」を受賞しています。

＊ ラック、LAC、JSOCは、株式会社ラックの国内及びその他の国における登録商標または商標です。
＊ その他、記載されている会社名・団体名、製品名などは、各社の登録商標または商標です。

この件に関するお問い合わせ

■ 掲載記事のお問合せ先には、こちらをご紹介ください。
株式会社ラック
Tel： 03-6757-0113（営業）　E-mail： sales@lac.co.jp

■ 本件に関する取材のご要望は、こちらにご連絡ください。
株式会社ラック　IR広報室　広報担当
Tel: 03-6757-0107（広報部門）、03-6757-0130
E-mail: pr@lac.co.jp　　Twitter： @lac_security
Facebook：　https://www.facebook.com/Little.eArth.Corp

※ラックのプレスリリース配信をご希望の報道機関の方は、メールにてお問い合わせください。
