平成 28 年８月２日

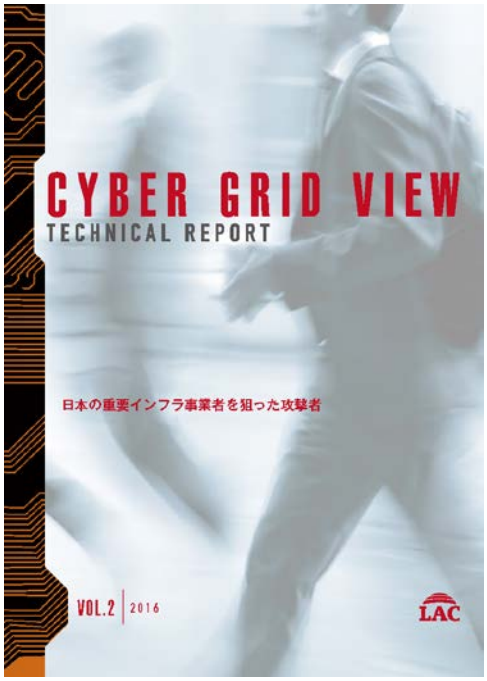
各位

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、追い続けた「Daserf」の実態レポート「日本の重要インフラ事業者を狙った攻撃者」を公開

## ～日本の重要インフラ事業者を執拗に狙う攻撃者の手法と、プロファイリングを技術情報にまとめて提供～

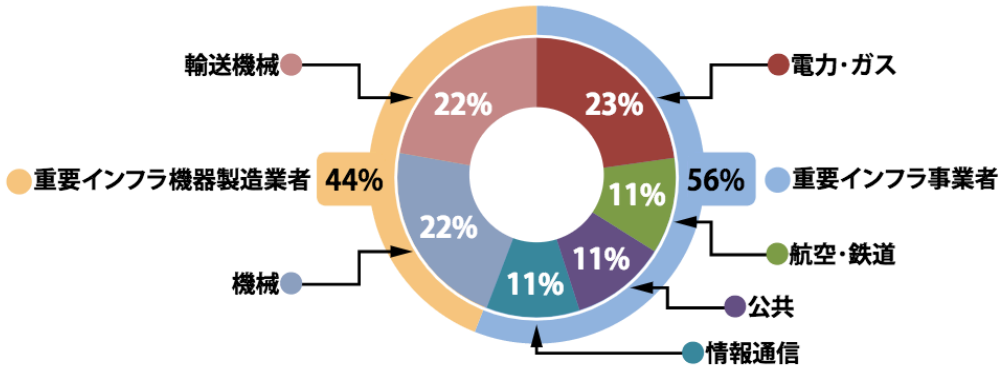
株式会社ラック（本社：東京都千代田区、代表取締役社長：髙梨 輝彦、以下ラック）は、標的型攻撃に関する調査レポート「日本の重要インフラ事業者を狙った攻撃者」を公開します。本レポートは、ラックの研究部門の一つであるサイバー・グリッド研究所の研究者が2013年より追跡調査している不正プログラム「Daserf：ダザーフ」について技術的な解説を行いました。さらに、「Daserf」の攻撃の痕跡から得られた情報を元に攻撃者の背景推測（プロファイリング）を行っており、セキュリティ対策に必要なサイバーインテリジェンス（対応能力）に寄与します。




サイバー・グリッド研究所では、高度な知見を有する研究者が国内で発生した攻撃事案や各種公開情報等を集積し、日々調査・分析しています。そうした研究活動を行う過程で、複数の被害に共通した痕跡が発見されることがあります。今回公開した CYBER GRID VIEW Vol.2 「日本の重要インフラ事業者を狙った攻撃者」もその一つで、 2013年1月に初めて調査を行った不正プログラム「Daserf」に関して取り上げて技術的な解説と攻撃者の背景推測（プロファイリング）などの結果を紹介するほか、「Daserf」が残す痕跡に関する情報についても参考情報として公開します。

本レポートの要約

- 「Daserf」を悪用する攻撃者は、日本の重要インフラに関連した組織を狙っていると考えられます。




ラックが対応した標的型攻撃事案のターゲット組織

- 「Daserf」の被害を受けた企業は、発見までに数カ月から2年半の時間を要しており、発見されにくい工夫がされていました。
- 「Daserf」は、遠隔操作機能を備えた高機能な不正ソフトウェアであり、指令サーバーの約65%は韓国企業が保有しているIPアドレスでした。
- 「Daserf」を悪用する攻撃者の背景推測（プロファイリング）を説明しています。
- 攻撃に関する痕跡情報（Indicator of Compromise）を掲載しています。

レポートの詳細とダウンロードは次のURLでご確認いただけます。
http://www.lac.co.jp/security/report/2016/08/02_cgview_01.html

「CYBER GRID VIEW Vol.1」はこちらをご確認ください
http://www.lac.co.jp/security/report/2014/12/16_cgview_01.html

ラックは、今後も引き続きサイバー・グリッド研究所の研究成果を防御や対処等に活用するほか、積極的に情報を公開し、社会全体のセキュリティレベルの向上に貢献できるよう努めてまいります。

以上

【 株式会社ラックについて 】　（http://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、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/

---