平成 28 年２月１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広報部長　岩　﨑　　勝
電　　話　０３－６７５７－０１０７

# 遠隔操作ウイルスへの指令伝達にDNSの仕組みを悪用した事案に関する注意喚起

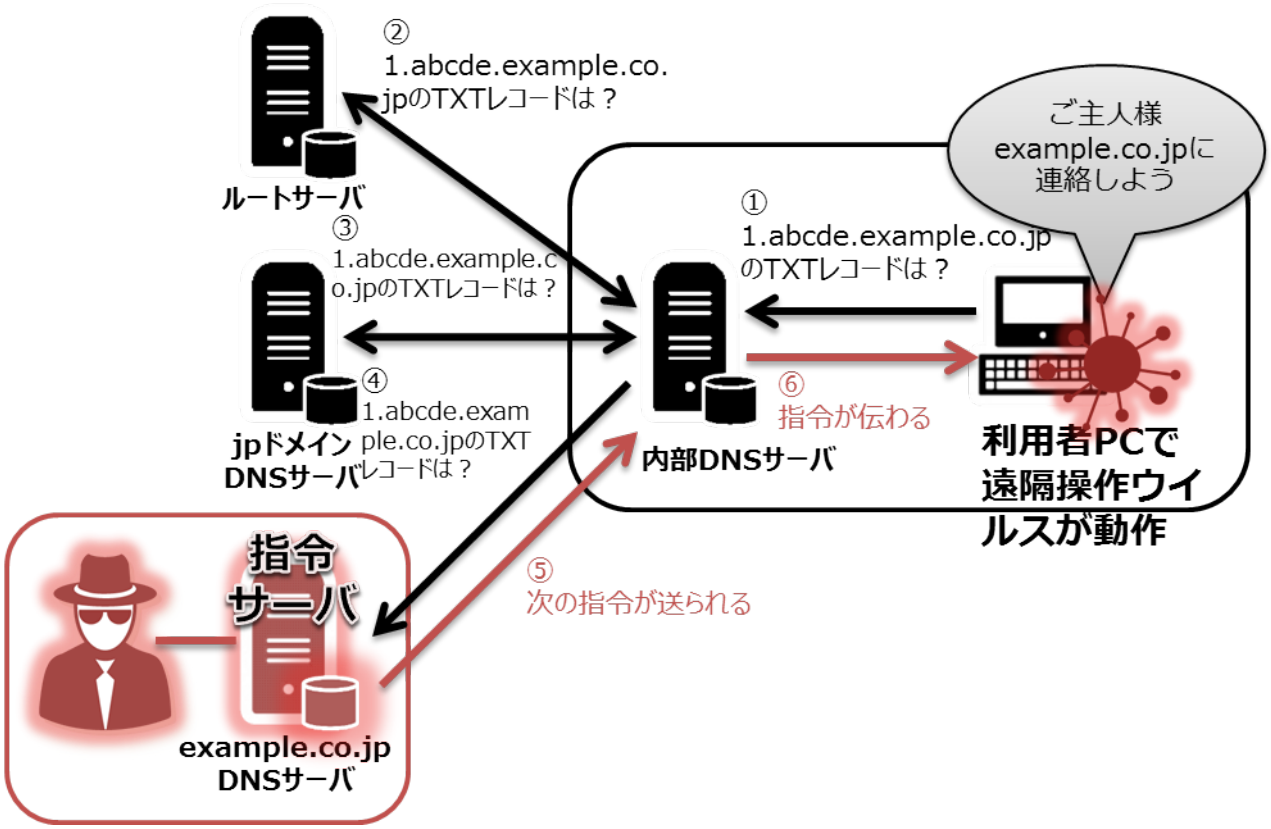
## ～情報セキュリティ対策の盲点を突いた攻撃方法に対する理解と、対応策について～

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、緊急対応サービス「サイバー119」で調査した複数の案件で、企業内部で暗躍する遠隔操作ウイルスに対する指令の伝達手段としてDNSパケットを悪用する事案を初めて確認し、注意喚起情報として公開しました。

ラックが運営する緊急対応サービス「サイバー119」は、お客様の要請を受け、年間350件以上のサイバー攻撃に関する調査・対応を行っております。昨年後半に複数の大手企業様より、PCで不審なソフトウェアが動作していることが確認されたことによる調査依頼がありました。ラックのフォレンジック担当者が問題のPCを調査した結果、企業内の情報を盗み出す目的で使用される遠隔操作ウイルス（RAT:リモートアクセスツール）であることが判明しました。

この遠隔操作ウイルスを解析したところ、攻撃者との指令伝達にDNS(Domain Name System)の通信を使用するDNSトンネリングとも言われる手口であることが確認されました。ラックが緊急対応した事案でこの手口が使用されたケースは初めてです。

攻撃者は、DNSサーバを模した指令サーバ(C2サーバやC&Cサーバとも呼ばれる)を構築し、企業内部で活動する遠隔操作ウイルスが、通常のDNS要求を模したリクエストを指令サーバのドメインに送り、指令の伝播を実現していました。




今回確認されたDNS通信による指令伝達には、以下のような深刻な特徴があります。

- DNSは、インターネット接続を実現する重要な技術で、DNSサービスはPCやスマートフォンなどインターネット接続機能を持つ機器であれば必ず使用しなければならず、影響を受ける可能性のある機器が非常に多い。
- DNSサービスへのアクセスを防ぐには、攻撃者が用意したDNSサーバのドメイン名を知る必要があるうえに、ドメイン名を知っていてもそのアクセスの制限は容易ではない。
- DNSサーバを企業内部のネットワークに構築していても、DNSの動作の履歴をログとして記録することはほとんどの企業で行っていないため、不正なDNSアクセスについて把握できない。
- Webブラウザやメール、メッセンジャーなどのアプリケーションを制限した業務端末であっても、遠隔操作ウイルスが実行できる機器であればDNSプロトコルを介して遠隔操作される危険がある。

以上のことから、本件の対応は困難ですが、少なくとも遠隔操作ウイルスが不正なDNS通信を行っているか否かを調査し、不正な通信が発見された場合には、速やかに遠隔操作ウイルスの対策を行う必要があります。

本件に関する技術的な説明と、対策の方法の詳細は注意喚起本文をご確認ください。

遠隔操作ウイルスの制御にDNSプロトコルを使用する事案への注意喚起
http://www.lac.co.jp/security/alert/2016/02/01_alert_01.html

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。2015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、「日本市場マネージドセキュリティーサービス プロバイダー最優秀賞」を受賞しています。



---

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広報部　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/

---