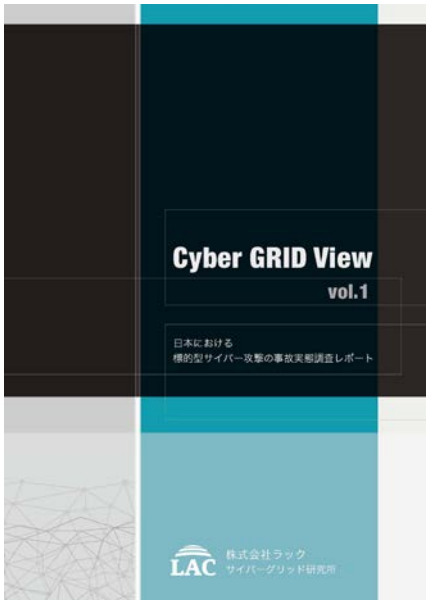
平成 26 年 12 月 16 日

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

ラック、日本で発生した標的型攻撃に関する実例と、複数事案の関連性を国内初公表
～豊富な実績を有するセキュリティ事故救急センターだからこそ解明できた、攻撃者の狙い～

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、自社のサイバー救急センターが緊急対応や情報漏えい事故調査で得た情報をサイバー・グリッド研究所にて分析した、「日本における、標的型サイバー攻撃の事故実態調査レポート」を公表します。本レポートは、特定企業や組織を狙い撃ちにした巧妙なサイバー攻撃である「標的型攻撃」について、国内で実際に発生した約 80 件の実例を調査・分析し、判明した事実を解説した日本初の技術レポートです。併せて、複数の標的型攻撃の関連性についても解明を試み、その一端を紹介しています。



「標的型攻撃」とは、米国 Google 社に対して密かに行われ、2010 年 1 月に報道されて世界的に話題となったサイバー攻撃の手法です。コンピュータウイルスを無差別にばらまく従来の攻撃方法ではなく、既存のウイルス対策ソフトでは検知できないウイルスを作成して行われます。侵入の手口は、メールへの添付や、罠をしかけた Web サイトへの誘導によって、相手に気付かれないように攻撃してきます。標的型攻撃では、ウイルスは何年もの間、標的となる企業内に潜伏して、情報や金銭の窃取、破壊工作などを行おうとする非常に悪質なサイバー攻撃なのです。

日本においても、企業や政府関係組織が被害を受けたことが 2011 年後半に報じられ、現在では日常的にこのサイバー攻撃が行われている状態になっています。

当社は、情報セキュリティのリーディングカンパニーとして、セキュリティ事故への緊急対応を支援する「サイバー救急センター」を運営しています。コンピュータインシデントの事故対応専門組織として 2004 年に業務を開始して以来、出動件数は 1000 件近くに上り、国内最多の事故対応実績を更新しています。近年、サイバー救急センターにおいても、標的型攻撃に関する調査要請を受けることが増えており、攻撃に関する技術的な手法の解析が進んでいます。また事故対応を行う過程で、一見全く関係のない複数の事案が同じ攻撃者によるものであったり、得られた情報に意図的な悪意を発見したりするなど、関連性が浮かび上がっています。

◆本レポートの特徴

・当社が調査した約 80 件もの標的型サイバー攻撃の被害事案をもとに、技術的なポイントと攻撃者の攻撃手法の傾向、事案間に共通して見られる事実を解説しています。

・攻撃に使われるツールは、一般的に流通していないものや流通するツールでも手が加えられたもので、ウイルス対策ソフトによる検出を回避しようとする意図が見て取れます。また、最新の攻撃手法も常に取り込んでいることがうかがえます。

・複数の標的型サイバー攻撃の痕跡から、同一の攻撃者が異なる企業を同時に狙っていたことが確認されました。これは多くの企業の被害調査を手がける当社だからこそ突き止められた事実です（下図参照）。

・調査で発見されたマルウェアの通信先コンピュータの IP アドレスなどが、既に調査済みの事案のものと同一だったことから、感染原因も同一であると類推し、早期解明につながったケースもありました（丸で囲った部分）。過去の攻撃の痕跡を蓄積していくことで、万が一の際も対策が早期に講じられると期待できます。

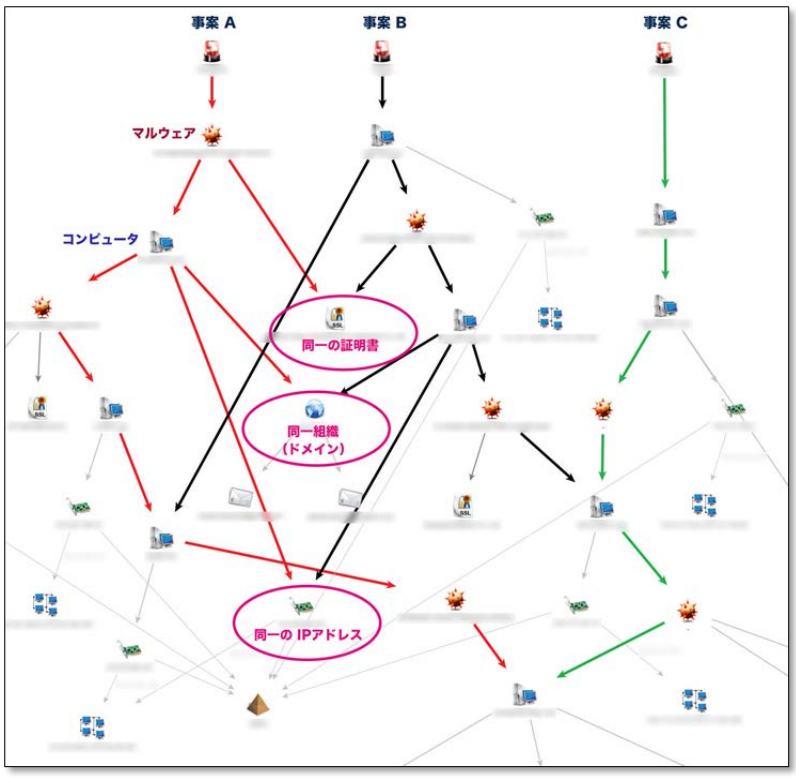


図　感染手段の異なる事案の関連

図は、異なる３つの組織で発生した標的型攻撃について、それぞれ調査を進めた結果、関連性が確認

されたことを表しています。A（赤）、B（黒）、C（緑）の３事案の調査で明らかになったもののうち、複数の色の矢印が示す先が確認された関連事項です。丸で囲った部分は、事案 B で発見されたマルウェアの通信先コンピュータの IP アドレスや、マルウェアに付けられた証明書などが事案 A のものと同じだったことを示しています。

このようなサイバー救急センターでの解析情報のほか、組織内からの情報流出・情報漏えいの可能性を評価する情報漏えいチェックサービスなどで得られた情報を当社のシンクタンクであるサイバー・グリッド研究所が詳細に分析し、攻撃の手口と複数事案の関連性について、今回、初めて総覧できる形にまとめました。

本レポートにより多くの企業が標的型攻撃の脅威を認識し、より実践的なセキュリティ対策の推進にお役立ていただけることを期待しています。

本レポートは、当社 Web サイトから無償でダウンロードできる形で提供いたします。

「日本における、標的型サイバー攻撃の事故実態調査レポート」

http://www.lac.co.jp/security/report/pdf/20141216_cgview_vol1_d001t.pdf

■ 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、1995 年にいち早くセキュリティ事業を開始。2012 年４月にグループの合併により、株式会社ラックとして新たにスタート。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、豊富な実績を誇る「脆弱性 診断サービス」、日本最大級の「セキュリティ監視センターJSOC」による 24 時間 365 日のセキュリティ監視・分析サービス、情報漏えい事故などの緊急対応・支援をする「サイバー119」の提供をはじめ、金融機関向け基盤システム開発で培った「システム開発」など、官公庁・企業・団体等のお客様に IT トータルソリューションサービスを提供しています。

【お客様からのお問い合わせ先】	【報道機関からのお問い合わせ先】
株式会社ラック Tel: 03-6757-0113　E-mail: sales@lac.co.jp http://www.lac.co.jp/contact/index.html	株式会社ラック　広報担当 Tel: 03-6757-0130　E-mail: pr@lac.co.jp

以上