日本の自動車業界における サイバー攻撃対象領域について

世界第3位の経済大国である日本は、それゆえ、サイバー犯罪の標的になりがちであるとも言えます。金融サービス、通信・メディア、製造業など、さまざまな産業のグローバルな中心地として機能する日本へ攻撃は、日本国内の企業や組織にとどまりません。グローバルに展開する日本企業には海外子会社も多数あり、サイバーセキュリティの専門家から、重大なリスクとなり得ると指摘されています。

世界的に名の知られたブランドを擁し、世界中に子会社を多く持つ、日本の自動車産業はその例の一つです。Rapid7の最新のレポートでは、日本国内の攻撃状況の全体像をについて説明しています。本ドキュメントでは、特に自動車業界を中心的に当社の研究者が分析を行った結果明らかになった脅威の主な傾向と調査結果をいくつかご紹介します。

「商品」のセキュリティに対する脅威

日本車は世界各地で製造・販売されているため、商品としての車自体のセキュリティ、知的財産、車両情報の保護は、安全性における重要な要素となります。

Rapid7の調査では、特に海外子会社に起因する侵害例が多数取り上げられています。それらの侵害では、車両情報や技術関連の知的財産情報が漏洩し、販売されています。

例えば、攻撃者「Oleg-Maslov」が、ディーラー診断ツールであるToyota Techstreamの盗難コピーを販売しています。こうしたツールを悪用した脅威アクターが、攻撃の対象とする車両の偵察を行い、情報を収集する可能性もあるのです。別の例では、多くの日本車ブランドを含む主要自動車メーカー数社に対応したキーレスエントリーシステムを悪用する自動車盗難ツール「AgentGrabber」が犯罪フォーラムで販売されていることを確認しています。

顧客データの侵害

個人情報（PII）は、サイバー攻撃者が狙うデータの種類としてよく知られています。自動車関連企業の顧客データには、住所、氏名、メールアドレス、加えて個人に販売された車両のVIN番号に関する情報が含まれることもあり、こうしたデータが、不正な信用枠の作成など、個人情報の悪用に使用される可能性があります。

過去数年間で見られた自動車業界での侵害には、日本の大手自動車ブランドのディーラーや販売子会社を対象とした侵害もあり、これらのディーラーが保有する数百万人の顧客のPIIのが攻撃者に侵害・収集される結果となりました。ある例では、サードパーティベンダーが侵害されたことに起因し、490万人を超えるホンダの顧客のデータ（氏名、メールアドレス、VINの一部またはすべて）が攻撃者に漏えいしています。

ビジネスメール侵害（BEC）

自動車製造企業は、世界最大級の企業と同等の価値を持つ、日本経済の主要な構成要素です。そのため、ビジネスメール攻撃の標的にもなり得ます。攻撃者は、ソーシャルエンジニアリングを駆使して騙し取った正規のメールアカウントを通じて、役員や社外の重要人物になりすまし、ターゲットに送金を促すメールを送るのが一般的です。

ここでは、日本の自動車業界に対する攻撃の影響のごく一部をご紹介しました。同セクターを始め、他のいくつかのセクターに関する詳細な分析については、レポートをご覧ください。