PwC's Cyber Intelligence

自動車産業をターゲットにするサイバー攻撃

中国の一帯一路構想に呼応する脅威アクター

サイバー攻撃では情報量や対象範囲の広さの差から攻撃者が有利な状況であり、CISOなどのセキュリティ担当責任者は、より積極的なサイバー攻撃への防御戦略を策定しなければなりません。PwC's Cyber Intelligenceでは、今後のリスク要因の特定を支援するため、スレットインテリジェンスとその背景にある攻撃者の動向を解説します。

サイバー攻撃の動機は社会経済活動と連動

近年、国家の経済政策と関連し、長期にわたり計画的に行われるサイバー攻撃が世界で増加しています。いわゆる高度で継続的に脅威を与えるAPT（Advanced Persistent Threat）を他国に仕掛けることで技術情報などを盗み出し、経済的な便益につなげようとする試みです。これらは必ずしも当該国自身あるいは関係機関の犯行とは言えません。当該国に情報を売りつけるために他国の情報を盗むハッカー集団も存在するからです。

ここ数年、日本の自動車メーカーおよびその関連企業はサイバー攻撃の標的となっている可能性が高いです。国内組織が標的となるだけでなく、海外の現地法人や工場も攻撃を受けています。一見すると無差別かつ広範に攻撃が行われているようですが、果たして本当にそうなのでしょうか。

現代は軍事や政治、経済や文化などの情報が国家間の競争に密接かつ統合的に活用されています。APTが観測された場合、社会経済的な動きと連動している可能性が高いです。そのため、まず攻撃の背景にある社会経済的な変化を整理します。

技術革新を強く推進する一帯一路の進展

世界の経済を牽引している中国は、アジアと欧州をつなぐ陸路および海路での物流ルートを作り、貿易を活性化させる取り組みである一帯一路を通じて、新興国の市場を活性化しています。中国は一帯一路を提唱して以来、すでに125の国と29の国際機関との間で計173の契約を締結しており（＊1）、日本企業が海外で活動する場合、一帯一路と無関係でいることはもはや難しい状況です。

さらに中国は一帯一路に含まれる「デジタル・シルクロード構想」に基づき、アジアとアフリカを結ぶ海底ケーブルを敷設したり、測位衛星を打ち上げたりと、デジタル化推進の旗振り役としても存在感を示しています。現在、世界で最も多くの測位衛星を保有しているのは中国です。北斗衛星導航系統（北斗衛星測位システム）と呼ばれ、多くのスマートフォンやカーナビゲーションなどで利用されています。次世代通信規格である5Gは中国企業が市場を占める割合が高い状況にあり、また中国企業が主導するeWTP（Electronic World Trade Platform）と呼ばれる国際電子商取引のプラットフォームや中国人民銀行による中央銀行デジタル通貨（CBDC：Central Bank Digital Currency）の整備も着々と進んでいます。日本企業が世界市場を相手にすることは、中国と接点を持つことと言っても過言ではないでしょう。

出典：＊1
China's Digital Silk Road: Strategic Technological Competition and Exporting Political Illiberalism（2019年8月1日、Pacific Forum）
https://www.pacforum.org/sites/default/files/issuesinsights_Vol19%20WP8FINAL.pdf
China's Digital Silk Road: A Game Changer for Asian Economies（2019年4月30日、THE DIPLOMAT）
https://thediplomat.com/2019/04/chinas-digital-silk-road-a-game-changer-for-asian-economies/

自動車産業がサイバー攻撃を注意しなければならない理由

自動車産業においても中国の台頭は目覚ましく、2025年に販売台数において世界のトップ10に数社を食い込ませることを計画しています。自動車は情報インフラの一部として機能することが想定されており、中国のデジタル・シルクロード構想にとっても重要な要素です。加えて中国では高速道路を代替滑走路として使うことも多く、一帯一路関係国の道路と自動車を押さえることは、軍事的にも意味を持ちます。

自動車産業は今、2つの大きな変化に直面しています。1つはガソリン車から電気自動車(EV)への移行、もう1つは発展途上国の道路整備に伴う市場の拡大です。この2つの変化は、新興企業のシェア拡大など業界再編を引き起こすと考えられています。こうした時期に技術開発やマーケティング活動で市場をリードすることは重要であり、競合企業の情報を手に入れたいニーズが極めて高いと言えるでしょう。さまざまな産業の中でも自動車産業が特にサイバー攻撃への注意が必要な理由は、ここにあります。

近年の自動車産業においては、一帯一路に呼応すると思われるサイバー攻撃も観測されるようになりました。

モンゴルを例にとってみましょう。同国では一帯一路の一環である「中国・モンゴル・ロシア経済回廊」によって、高速道路などのインフラ整備が急速に進み、自動車市場が拡大しています。モンゴルの自動車市場では、これまでは韓国車と日本車が大きなマーケットシェアを有していました。これらを背景に、モンゴルや、韓国、日本をターゲットにしたサイバー攻撃が増加したと考えられます。

サイバー攻撃から分析する脅威アクター像

サイバー攻撃を背景及び他事象との関係性に着目して分析することで脅威アクターの特徴を知り、その由来を把握することができます。一帯一路の中で、モンゴル・ロシア・中国経済回路に関連する脅威アクターは、PKPLUG、TONTO、TA428などです。

PKPLUGは過去6年以上活動を続けている脅威アクターで、そのターゲットは一帯一路に関係ある地域やASEAN、中国内の自治区などです。TONTOのターゲットは韓国と日本、TA428のターゲットはモンゴルです。

TONTOとTA428はいずれも、中国由来の脅威アクターが、東アジア圏への攻撃でよく利用するRoyal Road RTF Weaponizer（8.t）と呼ばれるツールを利用しています。（図1）

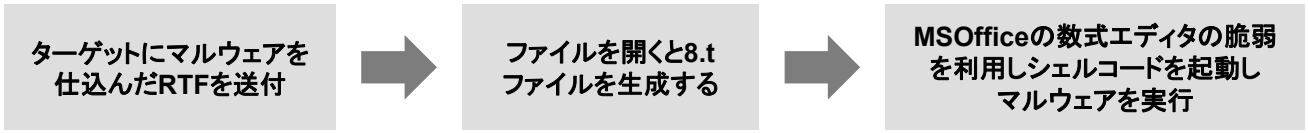

図1. Royal Road RTF Weaponizer 動作一例

このツールを利用する他のアクターはベトナム、アメリカ、フィリピン、ロシア、カンボジア、カザフスタンなどをターゲットにしています。これらのことから、上述のモンゴルに関連したサイバー攻撃も、中国の経済活動＝一帯一路と密接にリンクしていると考えられます。

とはいえ、全ての攻撃が国家やそれに呼応する脅威アクターによるものとは限りません。例えばベトナム由来のサイバー攻撃には民間企業の関与が疑われています。また、カナダの大学の研究機関に民間諜報企業が工作を仕掛けた事件では、その研究機関から批判を受けていた国の民間企業の関与が強く疑われています。国が関与せずとも、民間企業が民間諜報企業に依頼して情報収集や工作を行うことできる時代になっているのです。

社会経済活動とリンクしたサイバー攻撃を予知するには

経済活動とリンクしたサイバー攻撃は、中国だけでなくベトナムなどを拠点とした脅威アクターによるものも報告されています。現代においては経済活動の一部にサイバー攻撃が組み込まれていると言っても過言ではなく、特に新興国市場に参入する際には、企業は市場での競争だけでなく、サイバー攻撃にもさらされると考えたほうがよいでしょう。市場調査あるいはプロモーションを行うように、新興国の状況に合わせたサイバー攻撃への対策をあらかじめ講じることが、もはや必須となっています。

ではサイバー攻撃に対して、社会経済的要因を踏まえて、総合的に対処するために、企業はどのようなアクションを取ればよいのでしょうか。

重要なことは、技術や攻撃トレンドだけでなく、自社に関係する社会経済動向に注意し、呼応して発生し得るサイバー攻撃の可能性と脅威アクター、そしてそれに対する効果的な対処方法（サイバープレイブック）を事前に用意しておくことです。

自動車産業の場合は前述の通り、EV化や自動化と新興国での市場拡大という変化と、これとリンクしたサイバー攻撃に備える必要があります。注意しなければならないのは、攻撃を受ける可能性があるのは本社だけではない点です。自社製品がよく売れている国や、工場のある国で攻撃を受ける可能性もあるのです。

現地と日本本社とが連携し、攻撃を検知できない可能性がある箇所のリスクシナリオを想定し、モニタリングの強化をはじめとする対策を迅速に講じる必要があるでしょう。

今回のポイント

1
一帯一路参加国に進出している企業はサイバー攻撃へリスクが高まるとの認識のもと、攻撃シナリオの想定やモニタリング強化、サイバープレイブックの用意などが必要

2
本社だけではなく、工場や現地法人なども攻撃対象となる。現地と日本本社との連携の強化が必要

3
民間企業が主導するサイバー攻撃の動きにも注意が必要であり、幅広い脅威情報の確認が不可欠

執筆者

名和　利男

PwC Japan グループ
サイバーセキュリティ
最高技術顧問

林　和洋

PwCコンサルティング
合同会社
パートナー

岩井　博樹

PwC Japan グループ
スレットインテリジェンス
アドバイザー

村上　純一

PwCコンサルティング
合同会社
ディレクター

PwC Cyber Security & Privacy

https://www.pwc.com/jp/ja/services/digital-trust.html