日本を取り巻く脅威の現状

サイバー脅威レポート

Paul Prudhomme、主任セキュリティアナリスト

RAPID7

目次

はじめに

日本は、米国と中国に次ぐ世界第3位の経済大国です。多数のグローバル企業を生んだ国であり、こうした企業の存在を通じ、日本は他国の経済に大きな影響を及ぼしています。日本が経済的に果たす意義は大きいものの、自動車、製造、金融サービス、テクノロジー、メディア、通信をはじめとする日本企業に対するサイバー脅威に関して、海外で報じられる機会はあまり多くはありません。

本レポートは、自社データと第三者情報に基づいて日本国内を標的とした脅威に焦点を当てることにより、海外ではあまり知られることのなかった日本のサイバー脅威の状況を、諸外国にも伝えることを目的としています。Rapid7は日本の脅威状況に関して英語で発信し続けるJPCERTの研究者の業績に心から謝意を示します。

本レポートでは、日本国内の組織に対する脅威を関連業界別にまとめ、ランサムウェアと国家支援型脅威という、いくつかの業種で見られる2つの脅威の特徴に注目しました。経済的重要性の違いから、特定業種が、他業種と比較して、よりターゲットとなりやすい傾向にあります。例えば、日本の自動車業界は、日本経済と海外における活動の両方において大きな存在となっているため、国内企業を標的とした攻撃として記憶に残る攻撃の多くが、日本車メーカーを狙ったものであることは当然かもしれません。金融業界は諸外国においても狙われやすい業種ではありますが、日本もその例外ではありません。また、暗号通貨取引所をはじめとする暗号通貨関連企業も、旧来からの金融組織と並び、主な標的となりつつあります。国内におけるテクノロジー、メディア、通信業も、抱えるユーザーや業務内容、政府との関係などさまざまな理由から、攻撃にさらされています。

こうした脅威を取り巻く地域情勢は、日本国内に留まらず、海外事業、子会社、関連会社、さらに日本企業のその他の資産に広がっています。多くの日本企業が海外で非常に大きな存在となっているため、今回の調査では、対象範囲を日本国内のインシデントに限定しませんでした。海外の日系企業が侵害を受けた場合、内部ネットワーク経由の水平展開、認証情報の侵害やその他の手段を通じ、日本の親会社への攻撃にさらなる拍車がかかる可能性があります。日本の製造企業の部品を生産する海外拠点が、破壊的なランサムウェアや産業用制御システム（ICS）マルウェア攻撃に見舞われた場合、業務に支障が生まれ、サプライチェーンへの悪影響という形で親会社にも影響を及ぼす可能性があります。

日本企業に影響を与えるインシデントを対象としたあるレビューでは、その多くが海外子会社や関連会社の侵害から始まり、攻撃者が日本の親会社のインフラストラクチャへと水平展開していることが示唆されています。日本のある大手海運会社が2021年3月と6月に遭遇した2つの攻撃は、その最も顕著な例でしょう。どちらの攻撃も、攻撃者は海外子会社の侵害をきっかけとし、国内の海運会社のシステムにアクセスしたことが報告されています。

国内企業への侵害経路に海外子会社が繰り返し使用されることについては、2つの理由が考えられます。まず、海外子会社は、さまざまな要因により、セキュリティ監視が最適とは言えない場合があるという点です。例えば、新たに海外に関連企業などの資産を保有するような場合、同企業が既に持っていたセキュリティ問題が国内の親会社に入り込むなどのケースです。仮に親会社が支援して設立した海外拠点であっても、親会社の知らないうちに、望まない状況が生まれてしまう可能性もあります。大規模なグローバル企業の場合はさらに、ビジネスの多様さ、テクノロジー、法律、規制をとりまく環境、時差、言葉の壁など、コミュニケーションと調整の最適化を阻むさまざまな障壁にも直面することになります。

2つ目の理由として考えられるのが、言葉の壁です。攻撃者にとっては、条件が同じであるならば、わかる言語を使っている標的の方が、ソーシャルエンジニアリング攻撃を仕掛けたり、データを活用するのが簡単なため、母国語を使う標的を好んで狙います。**日本語人口は少なくないものの、そのほとんどは国内に在住しています。**英語など、広く使われている言語で事業を行う海外子会社は、日本語がわからない犯罪者にとって、言語的によりアクセスしやすく、好まれる標的となり得るのです。

ランサムウェア

ランサムウェアは世界中の組織にとって大きな脅威であり、国内においても例外ではありません。実際、かなりの数の国内組織がにおいて被害が発生していることから、ランサムウェアは、その他の脅威とは別に検討するべきかもしれません。

自動車製造業をはじめとする製造業は、日本経済において非常に重要な位置を占めており、これがランサムウェアリスクにさらされる危険を高めることにつながっています。事実、本レポートでの調査対象となった、自動車業界を除く国内製造業に影響を及ぼしていたインシデントの大半が、ランサムウェアに関するものでした。国内製造業を狙う攻撃者の多くは、ランサムウェアを使用するほか、入手した標的のアクセス権をランサムウェア実行者に販売するなどしています。製造業が保有する情報には、詐欺に活用したり他の犯罪者に販売することで収益を上げることが難しいようなものが多いため、直接窃取するのではなく、データを暗号化して身代金要求するほか、窃取したデータを公開すると脅すことでさらなる身代金をせしめる手法を取る場合があります。また、製造業は工場等の製造業務の中断やダウンタイムを嫌うため恐喝に屈しやすいと考えられているため、ランサムウェア実行者たちにとって格好の標的となりやすいとも考えられています。

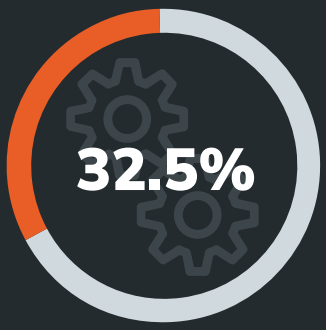
例えば、2020年6月にランサムウェア攻撃を受けたホンダは、インシデント対応中に、同社のカスタマーサービス、金融サービス、一部の製造業務に混乱が生じました。このインシデントでは、攻撃者が明確にホンダを狙って攻撃を仕掛けています。インシデント発生と同時期に、国内のとあるIPアドレスから送信された、あるSnake / EKANSランサムウェアが、ホンダの内部ネットワークドメインを積極的に検索し、ファイル暗号化プロセス引き起こそうとしていたことがその証拠です。自動車メーカーを標的としていることから、この攻撃者は、混乱を恐れた企業が簡単に支払いに応じることを見越していた可能性が伺えます。Snakeは、一部のICSプロセスを強制終了させるという点で、ランサムウェアの中では珍しい種類です。この攻撃で、ICSプロセスを強制終了させたのか、あるいは実際にホンダの製造業務の混乱を引き起こしたかどうかは明らかになっていません。

ホンダがランサムウェアの被害を受け、製造業務に混乱を起こしかねない状況に陥ったのは、同インシデントが初めてではありませんでした。2017年にWannaCryランサムウェアが世界的に感染拡大した際、ホンダ、日本の自動車メーカーの日産、フランスの自動車メーカーであるRenaultにも被害が及びました。WannaCryは実際に、各社の製造業務の一部に混乱を招くことに成功しています。

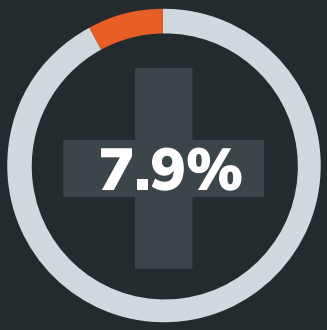
ランサムウェア攻撃がサプライヤーを狙って混乱を生じさせることで、間接的に自動車製造業本体を混乱に巻き込ませることもあります。例えば、2019年9月から10月にかけて、Subaru of Indiana Automotiveは、「サプライヤーの問題」とランサムウェアのインシデントを理由に製造業務を一時的に停止しました。2021年12月には、トヨタグループ傘下のある日本の自動車部品メーカーが、Rookランサムウェアオペレーターによるランサムウェア攻撃を受け、1.1TBのデータが侵害されたと主張しています。同社は、この攻撃による日本国内の資産への被害はほぼないものの、メキシコの製造施設で感染が発生し、従業員個人を特定できる情報（PII）が侵害された可能性があると報告しました。

警察庁（NPA）は、2022年上半期に国内で報告されたランサムウェア攻撃被害の32.5%が、製造業で発生したとしています。これは、最もランサムウェアに狙われやすいとされる医療業界の数値（同調査では7.9%）と比較しても、非常に高い割合です。攻撃ベクトルがわかっているランサムウェア攻撃の多くでは、VPNもしくはリモートデスクトッププロトコル（RDP）を経由して標的に侵入を果たしています。

ランサムウェア：日本ではヘルスケアよりも製造業が攻撃の標的に



2022年上半期に報告されたランサムウェア攻撃のうち製造業での割合



同期間にヘルスケア業界で報告されたランサムウェア攻撃の割合

出典：警察庁

Rapid7の研究では、2022年後半から2023年初頭の時点で、LockBit 3.0ランサムウェアオペレーターが国内組織の全般、特に製造業を標的にしていることが明らかになっています。海外製造業の多くは日本国内から部品供給を受けているため、日本国内の製造業者を狙ったランサムウェア攻撃は、世界中の製造サプライチェーンに影響を与え、混乱を招く恐れがあります。例えば、2022年10月に、LockBit3.0を使用した攻撃者が、国内製造業者である大宮化成を侵害したと主張しました。同社は、自動車、製造、通信、半導体、ヘルスケアなど、複数業界の組織のサプライチェーンを支えています。この攻撃では、身代金を支払わなければ侵害したデータを開示する、という脅迫が発生しています。

LockBitランサムウェアを使用した攻撃者が国内製造業を標的にしたのは、この2022年後半から2023年初頭のキャンペーンが初めてではありませんでした。Rapid7の研究者は、2020年9月の時点ですでに、初代LockBitを使った攻撃者が、産業用ロボット、サーボ、モーションコントローラー、ACモータードライブ、スイッチを製造する国内製造業を侵害して窃取したと言われるデータが開示されていたことを確認しています。

2020年以降、Rapid7は、国内製造業を標的としたランサムウェアデータの開示と脅威の事例を確認し続けています。データ開示を伴う恐喝は、製造業を対象としたものを含むランサムウェア攻撃における一般的な手口となりつつありますが、製造業が保有する一部の情報は、その性質上販売などを通じて金銭化しにくいものであることが多いことから、攻撃者は情報窃取後公開すると脅して金銭を巻き上げるしかないケースがあります。実際に、攻撃の中にはファイルの暗号化をまったく行わず、侵害したデータを公開すると脅迫するだけのものもあります。

Panasonic Indiaでは、2020年10月にデータを開示すると恐喝する被害が発生し、実際に4GBを超える機密データが開示されました。このインシデントでは、ロシア語を操る攻撃者が、「50万米ドルの身代金を支払わねばデータを公開する、身代金の支払いを拒否した場合侵害されたデータと不正なネットワークアクセスを他の犯罪者に4万米ドルで販売する」と恐喝しました。開示されたデータには、銀行口座番号、会計に関する記録、認証情報に加え、ベンダー、顧客や従業員に関する情報が含まれていました。その後、2022年2月に同社のカナダ事業でも別のランサムウェア被害が発生し、ランサムウェアContiを利用した攻撃者が、侵害により取得したとする人事記録や会計記録などのデータを漏えいさせました。

同様に、2017年12月、日産、INFINITI、三菱のディーラーからの自動車の購入・リース資金の提供を行うNissan Canada Finance（NCF）では、攻撃者がNCFの顧客データの一部を実際に窃取したデータのサンプルとして示した上で、身代金を支払わない場合はデータ全体を開示すると脅迫する事案が発生しています。NCFが調査を実施した結果、侵害の証拠は発見されず、社員が顧客データへの正規のアクセス権を悪用し、恐喝を目的として故意に約30万人のデータを流出させたのではないかと見られています。

しかし、ファイルの暗号化とデータ開示恐喝を行う攻撃の方が一般的ではあります。2021年4月、ランサムウェアAstro Lockerを利用する攻撃者が、テクノロジー・ヘルスケア業界向けに光学製品を供給する国内メーカーを侵害することで窃取したとするデータを開示しました。公開された300GBのデータには、財務記録、生産の詳細、メール通信、患者データ、ネットワーク認証情報、安全性報告が含まれていました（図1）。

材料や部品を供給する在米日本企業子会社や支店も攻撃のターゲットとなっています。例えば、Rapid7の研究者は、2020年12月にランサムウェアDopplePaymerを利用する攻撃者が、三菱マテリアル株式会社の米国子会社、米国三菱ポリシリコンに対する侵害で取得したとするデータをの開示を確認しています。米国三菱ポリシリコンは半導体製造用のシリコンを生産しており、侵害されたデータのサンプルには、人事記録、請求書、会社のネットワーク上のマシン一覧が含まれていました。

2020年12月にも、Rapid7の研究者は、ランサムウェアNetwalkerを利用する攻撃者がNTN株式会社の米国子会社NTN Bearing Corporation of Americaの侵害で取得したとするデータの開示を確認しています。同社は、ボールベアリング、等速ジョイントなどの産業用・自動車用部品を製造しており、侵害されたデータには、財務記録、販売文書や従業員のPIIが含まれていました。

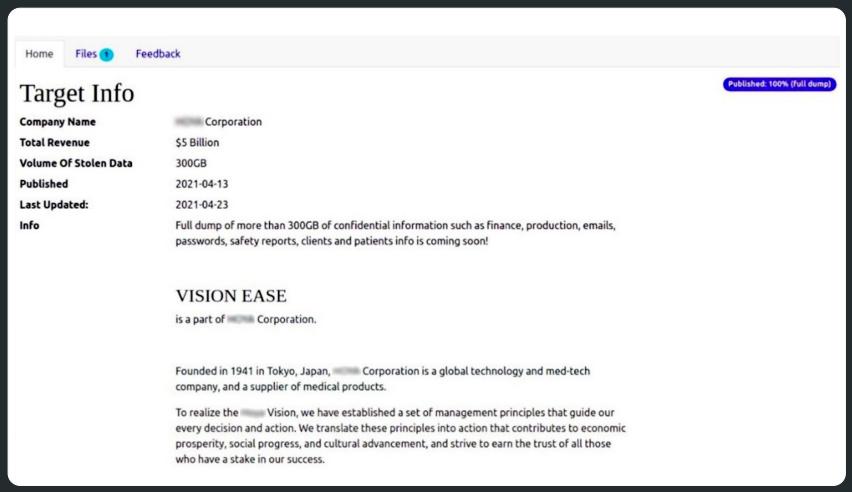


図1

国家支援型脅威

日本は、国家支援型脅威の標的ともなっています。歴史的、そして昨今日本との関係において緊張が高まる「お隣の国」である中国や北朝鮮、ロシアは、セキュリティ関係者が頻繁に対象とするサイバー攻撃を支援する国家ですが、政治的、外交的、軍事的要因を始めとする国家安全保障上の理由で日本が標的となる可能性が高まっています。高度に発展した豊かな日本経済は、知的財産（IP）の侵害や、暗号通貨などの金銭窃盗を通じた経済的な利益を目的とした攻撃者の標的になりやすいのです。

こうした状況を受けて、日本は2022年12月に国家安全保障戦略（NSS）を改定 し、従来の軍事防衛態勢とサイバー防衛態勢の双方を改善しました。今回の改定ではロシアのウクライナ侵攻が重要な要素となりましたが、中国の軍事力増大や北朝鮮の弾道ミサイル計画なども脅威とされています。改訂版NSSでは、敵対的海外政府の通常の軍事力に対してだけでなく、「ハイブリッド戦争」戦略の一部となる可能性が高いサイバー攻撃に対しても、より積極的な防御が必要であることを提言しています。

中国のサイバースパイ活動

中国のサイバースパイグループに共通する目的は、知的財産窃取です。中国の地域経済競争の相手国であり、また製造、自動車、テクノロジーなどの主要産業における貴重な知的財産を大量に保有する日本は、攻撃者の重要な標的となっています。例えば、「Earth Tengshe」または「Bronze Riverside」として知られる中国の国家支援型アクター、APT10による攻撃活動の一部は、2021年後半の「A41APT」キャンペーンで主に国内の製造、エンジニアリング、電子機器、自動車、エネルギー、テクノロジー企業とその海外子会社を標的としていました。セキュリティ研究者によると、同キャンペーンは国内親会社へアクセスするため、日本企業の海外子会社とサプライヤーを標的としたものであるとし、攻撃者が強固なセキュリティ対策を講じている国内の親会社への直接攻撃を避け、対策が手薄な海外子会社などに目を付けたものである可能性があるとしています。

APT10の関連グループ「Bronze Starlight」は、2021年半ばにIP盗難攻撃をランサムウェアやデータ開示の恐喝攻撃に偽装することで、IP盗難の新たな手口を作り出しました。これは、被害企業が攻撃の目的がIP窃取であることに気づきにくくする目的のものであると推測されています。Rapid7は、被害企業が攻撃の真の目的を理解することで、事業戦略を見直し、IPの競合他社への漏えいによる競争力低下を防止できると考えています。また、ファイル暗号化には過去のサイバースパイ行為のフォレンジック的証拠を隠蔽できる利点もあります。ランサムウェアのインシデント対応が、過去発生した情報漏えいへの対応を困難にする可能性があるのです。Bronze Starlightの攻撃対象となった国内企業には、電子部品の設計企業やメーカーなども含まれていました。

中国の攻撃者は、日本企業の中国子会社を踏み台として、国内親会社やクライアントを狙います。例えば、国内の報道によると、国内電子機器メーカーにおいて2019年に発生した侵害の背後には、中国のサイバースパイグループTick（別名「Bronze Butler」）があるとされています。同侵害により、日本の防衛および重要インフラストラクチャ組織など、官民両方のクライアントに関する情報が公開されました。この侵害は被害組織の中国の関連会社内から発生したものであり、攻撃者はこの関連会社のサーバーに対する侵害から、組織全体に侵入を拡大したとされています。攻撃者は、マルウェア検出ソフトウェアのゼロデイディレクトリトラバーサルと任意のファイルアップロードの脆弱性を悪用しました（CVE-2019-18187）。

この他にも、中国のサイバースパイグループLuoYuが2021年に国内テクノロジー企業の中国子会社に狙いを定め、独自のモジュール式バックドア、WinDealerを使った攻撃を仕掛けています。2022年半ば時点で、LuoYoは自動更新サービスを使ってWinDealerを標的に配信する「Man-on-the-Side（MotS）（別名Quantum Insert）」攻撃を開始しています。MotS攻撃は、クライアントとサーバー間の通信検出し、正規のトラフィックより先に不正な応答を行うものです。

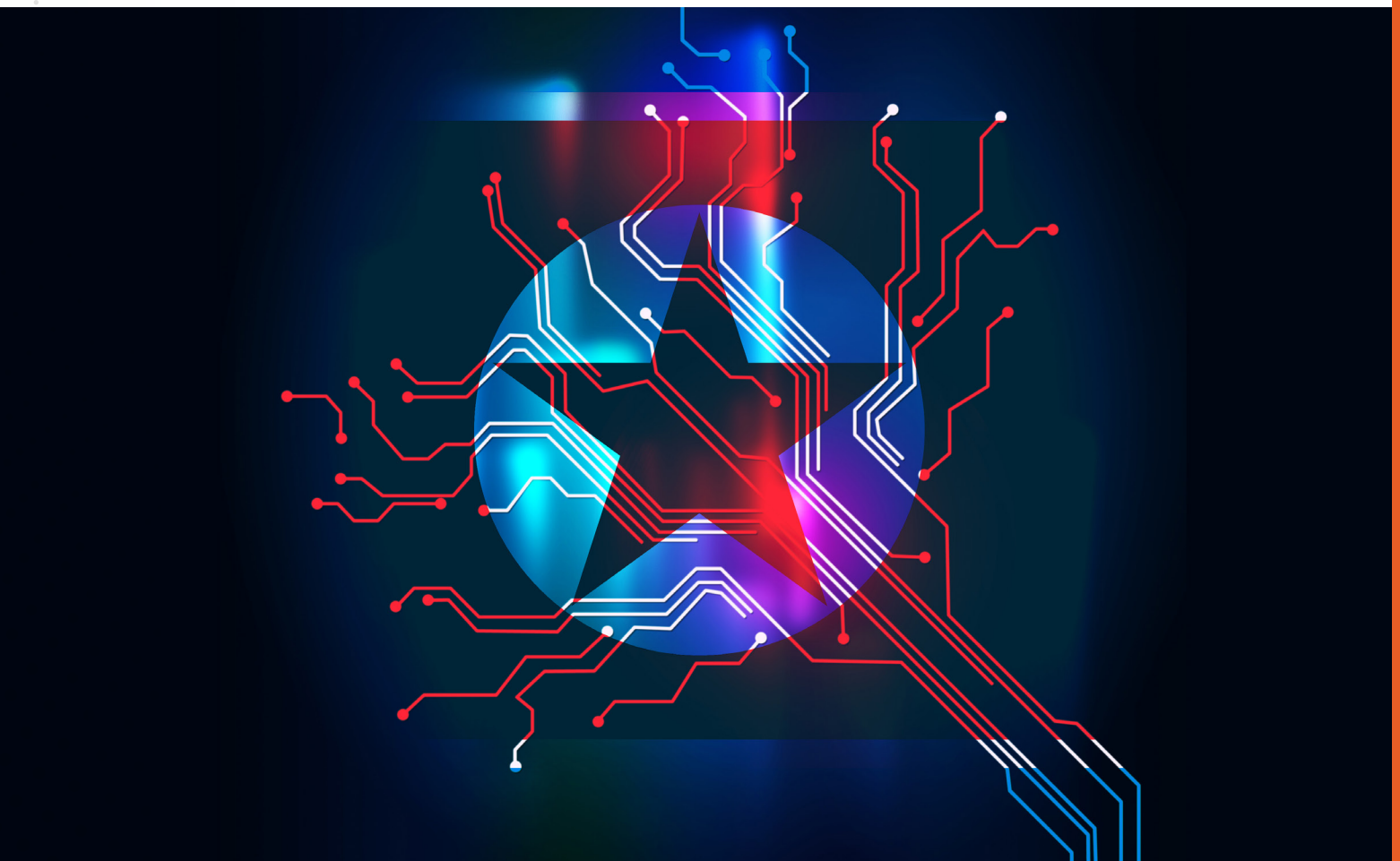
2021年3月には、日本企業の中国子会社経由で国内のデータが中国に公開されるリスクが話題になりました。チャットアプリLINEの中国の関連会社のエンジニアが、日本のサーバーを介して、氏名、電話番号、住所、メールアドレス、識別番号など、約8,600万人の国内LINEユーザーの個人データにアクセスしていたことが発覚したことが原因です。これに伴い、政府は関係者にLINEの使用を停止するよう命じました。

政治的、外交的、軍事的理由から、中国のサイバースパイは日本国と日本政府を重要な標的としています。報道によれば、中国のBlackTech関連の攻撃者は、2021年5月にクラウドベースのSaaS情報共有プラットフォームに対する侵害に関与した上、日本の官庁のデータを多数公開しました。同組織に対する捜査で、攻撃者は侵害した認証情報を使用して正当なトラフィックに紛れ込み、悪意のあるアクティビティを検知されないようにしていたことが明らかになりました。その狙いは、日本の原子力発電所と東京オリンピックに関する情報でした。BlackTechは過去にも、Flagproマルウェアを防衛、電気通信、メディア関連組織への攻撃で使用しています。つい最近では、2022年9月、日本の組織への攻撃でF5 BIG-IPデバイスの脆弱性であるCVE-2022-1388を悪用しています。

2022年6月から7月にかけ、中国の脅威グループMirrorFaceは、とある政党所属の政治家を狙った「Operation LiberalFace」スピアフィッシングキャンペーンを実施しました。MirrorFaceは、有名なアクターグループであるAPT10に属している、あるいは関係しているグループであると見られます。同グループは、これまでに日本の政治、軍事、外交、学術に関連する機関を標的としてきています。このキャンペーンは2022年7月の参議院選挙の前の日の夜に実行されたものです。とある政党を騙り、今回の選挙に特に言及したメールを送信しています。これらの不正メールを通じてMirrorFace独自のLODEINFOマルウェアが送られ、その結果、標的の認証情報やメール、ファイルなどのデータが侵害されました。注目すべきなのは、MirrorFaceが拡張子として「.jtd」を持つ、ジャストシステム社製一太郎のファイルを狙って収集していたことです。さらに、ジャストシステムの正当な実行可能ファイルに偽装した不正ファイルを使用し、LODEINFOに感染させようともしています。

北朝鮮とその犯罪活動

2022年10月、警察庁および金融庁は、北朝鮮の攻撃グループLazarusが国内暗号通貨取引所を攻撃したことを警告する声明を発表しました。同声明では、このインシデントは最近発生したとされていますが、それ以上の具体的な情報は開示されず、攻撃ベクトルとしてフィッシングとソーシャルエンジニアリングが使用されたことのみ言及されています。暗号通貨は、従来の金融機関以外で金銭を窃取する手段として、近年、北朝鮮の犯罪活動の格好の標的となっています。



Lazarus Groupは、2018年にすでに国内の暗号通貨を狙っていたと考えられます。国連（UN）の報告書は、2018年に発生した国内暗号通貨取引所、コインチェックの侵害が同グループによるものとしています。この侵害では、約5億3,300万米ドル相当の暗号通貨が窃取されました。具体的な侵害の手段は未だ不明ですが、コインチェックは、インターネットからアクセスできるために、オフラインで安全に通過を保管できる「コールドウォレット」と比較すると脆弱であるとされる「ホットウォレット」に盗まれた暗号通貨を保管していました。

暗号通貨が狙われる対象は、暗号通貨取引所だけとは限りません。Lazarus Group、Bluenoroffにより展開された2021年後半のキャンペーンでは、同グループが金融サービス、テクノロジー、金融テクノロジー（FinTech）を専門とする国内ベンチャーキャピタル企業になりすまし、暗号通貨を窃取しようと攻撃を仕掛けました。この攻撃では、国内のベンチャーキャピタル企業名を偽装する不正ドメインや、投資勧誘に関連する偽文書が使用されていました。

同じくBlueNoroffにより展開された2022年秋のキャンペーンでは、従来型の金融企業、特に銀行やベンチャーキャピタル企業が標的となりました。同グループは、このキャンペーンで偽のドメインを登録していましたが、その大半が国内金融機関名を偽装したものでした。このキャンペーンは、インターネットからダウンロードされたファイルをユーザーに警告しないよう、.isoや.vhdなどの珍しいファイル拡張子が使用されていました。不正ファイルに賞与グラフを思わせるものなどの日本語のファイル名を使用していることから、日本国内の金融企業を狙ったことは明らかです。

Lazarus Groupは、ランサムウェアからも収益を上げています。2021年4月、Lazarus Group配下のAndarielがMauiランサムウェアで最初に攻撃したのは、国内のある住宅会社でした。Mauiによるペイロードのコンパイル日とこのインシデント発生のタイミングを照らし合わせると、同企業が最初の被害を受けたことに間違いありません。Andarielは、2020年12月に同社のネットワークを侵害し、継続的にアクセスできるようにリバースプロキシツール3proxyを使用し、その後、3〜4か月の「滞在期間」を経て、DTrack偵察ツールを配備した後にMauiを展開しました。

Lazarus Groupは、独自の犯罪活動に加えて、IP窃取を始めとする従来のサイバースパイ活動も行っています。2022年初から半ばにかけて行われた、IP窃取を目的とした日本と北米のエネルギー組織に対する一連の攻撃も、同グループが背後にあったとされています。同キャンペーンは、VMWare Horizon Serversの脆弱性を悪用しています。初期アクセス権を取得した後、WindowsとLinuxに互換性があり、JPCERTにも記録されているLazarus Group独自のYamaBotマルウェアをインストールしました。

また、日本は政治的、外交的、軍事的理由から、北朝鮮のスパイ活動の標的ともなっています。2021年半ばには、北朝鮮を専門とする国内の防衛・メディア関係者に対する一連のフィッシング・マルウェアメール攻撃 が観測されています。ソーシャルエンジニアリングに使用された内容は北朝鮮に関するもので、北朝鮮のサイバースパイグループKimsukyのツールが攻撃に使用されていました。

ロシア・ウクライナ戦争

2022年9月、親ロシアのハクティビストグループ、Killnetは、日本の政府機関や民間企業のウェブサイトに対してDDoS攻撃を仕掛けたとの声明を発表しました。Killnetは、ロシアのウクライナ侵攻に関連し、ロシアに対して制裁などの対応を取った日本をはじめとする各国を標的としています。Killnetはロシアの支援を受けていることを否定しつつも、日本の「軍事的対応」を非難しているのは興味深い点です。

トヨタの部品サプライヤーに対する2022年2月のランサムウェア攻撃では、そのタイミングから、ロシアの関与が疑われました。この攻撃はロシアのウクライナ侵攻直後に発生し、トヨタが日本での製造業務を一時的に停止する原因となりました。これ以前にも駐日ロシア大使は、ウクライナ侵攻を理由としたロシアに対する国際制裁への参加に関して、日本に警告を発しています。真相は定かではありませんが、この製造停止はトヨタの子会社である日野とダイハツにも影響を及ぼたとされています。トヨタの「ジャスト・イン・タイム製造」は、日本製造業のビジネス文化を代表する方法論ですが、予備在庫を持たず、サプライヤーから納入した材料や部品を直ちに製造過程に移す必要があるため、サプライチェーンの混乱に対しては脆弱であると言えます。

ベトナムと外国の競合他社

ベトナムのAPT32（別名OceanLotus）は、新進のベトナムの自動車業界の競合となる外国メーカーを特に標的としています。日本のある大手自動車メーカーの関係者は、2019年にAPT32が同社とその海外事業を標的にしたことを匿名で明かしたとされています。セキュリティ研究者は、APT32が攻撃ベクトルとして同社を偽装するドメインを作成していることを観測しています。国内自動車メーカーの事業を狙ったのは、親会社のインフラストラクチャへのアクセス手段の獲得が目的だったとも考えられます。

特定国との関連が不明な脅威グループ：Earth Yako

日本を特に狙ったあるサイバースパイグループについては、一部の研究者が中国、韓国、ロシアの容疑者関与の可能性を指摘しているものの、その国を特定することが依然として困難なものもあります。「Earth Yako」は、少なくとも2021年10月から 公共、エネルギー、学術機関などの国内組織をターゲットにしており、「Operation RestyLink」キャンペーンでよく知られています。Earth Yakoは、東アジアにおける日本の外交に関連するソーシャルエンジニアリングコンテンツを使用し、不正な.lnkや.isoファイルを持つ.zipアーカイブを送信します。日本のIPアドレスを使用していますが、これは国内の発信元になりすますためと考えられます。その後の感染段階では、Cobalt Strike侵入テストフレームワークとオープンソースの C2フレームワークCovenantなどの既製のツールを使用し、侵害元の特定を避けています。Earth Yakoは、2023年1月の時点でも攻撃を行なっていました。

対象となった組織の業種

自動車産業

自動車産業は、日本を取り巻く脅威の中でも特に標的にされています。日本の自動車産業は規模が大きく、多くの企業が広く海外事業を展開しており、世界中の消費者に対するブランド力も相当なものです。自動車業界は、ランサムウェア攻撃などの製造業務を混乱させるインシデント、顧客データの侵害、ベンダーなどの提携先のサードパーティが侵害されることによって起こる自社データやシステムの被害、セキュリティの誤設定による脆弱性の増大など、さまざまな脅威にさらされています。

製品のセキュリティに対する脅威

車両自体と内部の技術を標的とする攻撃もあるため、製品のセキュリティは自動車メーカーにとって非常に重要です。アンダーグラウンドな犯罪フォーラムでは、日本車ブランドと日本車業界を対象とした攻撃に使用されるツールとテクニックが公開されています。例えば、2019年6月、Rapid7の研究者は、犯罪フォーラムのユーザー「Oleg-Maslov」が、ディーラー診断ツールであるToyota Techstreamの不正なアクセスの販売をしていることを観測しました。脅威アクターは、こうした正規のソフトウェアを悪用し、目的の車両を偵察したり、攻撃を計画するための情報を収集したりしている可能性があります（図2）。

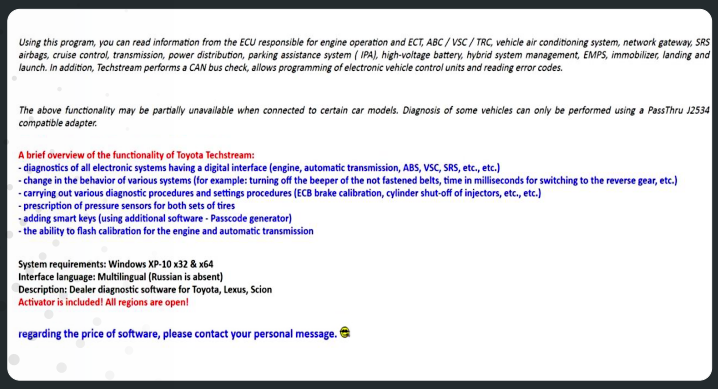


図2

図3

また、Rapid7の研究者は、2019年10月に自動車盗難ツール「AgentGrabber」がロシア語圏の犯罪フォーラムで販売されていることを観測しました。5,000米ドルで購入できるこのツールを使用することで、キーレスエントリーやキーレスゴーシステムを悪用して、ホンダ、トヨタ、スバル、マツダ、日産などの複数のメーカーの車両への不正アクセスと制御が可能になります（図3）。

顧客データの侵害

脅威アクターは、自動車会社への攻撃で個人情報の盗難や詐欺など、悪意のある目的で顧客データの窃取を狙うことがあります。2019年3月、トヨタ自動車は、国内のディーラーと販売子会社での侵害の発生で、310万人の顧客のPIIが公開された可能性があることを発表しました。同社は、公開された可能性のあるデータには支払いカード情報は含まれていないものの、氏名、生年月日、雇用に関する情報が含まれている可能性があることを強調しています。生年月日や雇用履歴などの情報は、ID窃盗犯が不正な信用枠を作成する際に役立ちます。ほぼ同時期に、タイとベトナムのトヨタ現地法人でもセキュリティインシデントが発生したとの発表がありましたが、それ以上の詳細は明らかにされていません。

カスタマーサービス業務も、自動車メーカーがベンダーにアウトソーシングするものを含め、メーカー外での消費者データ漏えい源となり得ます。2020年7月、南米の犯罪グループKelvinSecTeamは、ホンダを始めとする様々な自動車メーカーの車両所有者50万人にカスタマーサービスを提供するコールセンターを侵害し、アンダーグラウンドの犯罪コミュニティでこのデータへのアクセス権を販売しました。対象のPII（個人情報）には、氏名、メールアドレス、住所、車両登録の詳細が含まれていました。2010年には、新規登録されたホンダの顧客にメール送信したサードパーティベンダーへの侵害により、数百万人のホンダの顧客のデータが公開されています。侵害されたデータには、ホンダ顧客220万人の氏名、メールアドレス、VINと、ホンダ「アキュラ」所有者270万人のメールアドレスが含まれていました。

2020年7月

50万人

の車両所有者（複数自動車メーカー）のデータが公開された可能性。

2010年12月

220万件

のホンダ顧客のデータ（名前、メールアドレス、VINなど）が侵害。

2019年3月

310万件

のトヨタ顧客のPIIが公開された可能性。

2010年12月

270万件

のホンダアキュラの顧客のメールアドレスが公開。

設定ミス

セキュリティ設定ミスは、自動車会社だけでなく、あらゆる組織における脅威状況を悪化させる恐れがあります。例えば、2022年11月、トヨタではグローバルサプライヤー準備情報管理システム（GSPIMS）の脆弱性により、攻撃者がアカウントに関連付けられているメールアドレスを特定するだけで、ポータルのアカウントを侵害できることが判明しました。攻撃者は、トヨタのメールアドレス設定ルールを把握した上で、公開情報からサプライチェーンの職務上GSPIMSへのアクセスが必要となる可能性が高いトヨタの従業員の名前を割り出すだけで、簡単にその人のメールアドレスを推測することができてしまいます。同ポータルではJSON Webトークン（JWT）でユーザー認証を行っていましたが、メールアドレスのみを入力すれば良く、パスワードは必要ありませんでした。この脆弱性により、システム管理者アカウントを含むウェブサイトの全ユーザー14,000人に影響が及びました。

Rapid7の調査は、設定ミスを悪用した自動車ブランドへの他の攻撃事例も観測しています。例えば2021年1月には、インターネットに公開されたBitbucket Gitサーバーのユーザー名とパスワードが「admin/admin」となっていたことが発端となり、攻撃者によってNissan North Americaのソースコード約20GBがTelegramで公開する事態を引き起こしています。このソースコードには、同社のモバイルアプリ、ディーラービジネスシステム／ディーラーポータル、車両診断ツール、販売・マーケティングおよび顧客獲得・維持ツール、車載コネクテッドサービスのコードが含まれていました（図4）。

2021年1月

20 GB

の日産北米子会社のソースコードを攻撃者がTelegramで公開。

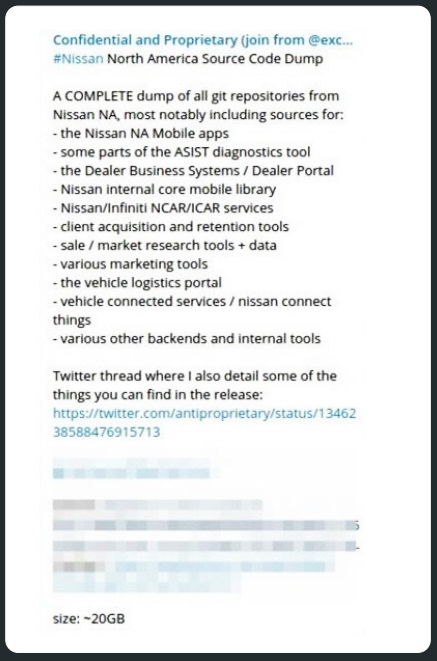


図4

また、2022年9月には、トヨタの車両管理アプリケーション「T-Connect」のソースコードが誤って公開されたことから、296,000人以上のユーザーが5年近くも攻撃のリスクにさらされていたことが明らかとなりました。T-Connectウェブサイトの開発を支援しているあるベンダーがソースコードをGitHubにアップロードし、公開状態のままにしていたことが原因で、このソースコードには、メールアドレスや車両管理番号などのユーザー情報を保存するサーバーへのアクセスを許可するキーが含まれていました。

ホンダでは、1年間にElasticSearchデータベースのセキュリティの設定ミスが2回発生しています。2019年12月、あるセキュリティ研究者は、ElasticSearchデータベース経由でホンダの北米顧客26,000人のPIIが誤って公開されていることを発見しました。このデータベースは、インターネット経由で誰でもアクセスできる状態であり、公開されたPIIには、氏名、住所、電話番号、メールアドレス、VIN、車両の詳細、車両サービス記録が含まれていました。別のセキュリティ研究者は、同社に関し、2019年7月に別のElasticSearchデータベースが公開されていることを確認しています。この件では、同社のCEO、CFO、CSOを含む世界中の約30万人のホンダ従業員に関する社内ネットワークの情報データベース40GBが公開されていました。公開された内容には、ホスト名、MACおよび内部IPアドレス、OSバージョン、パッチ適用およびエンドポイントセキュリティソフトウェアのステータスなど、ネットワーク侵入を手助けする可能性のある情報が含まれていました。特に目立つ名前の「uncontrolledmachine」というテーブルでは、エンドポイントセキュリティソフトウェアがインストールされていないマシンがリストアップされていました。

サードパーティのクラウドサービスの設定ミスには別のリスクも伴うことが、次のホンダの顧客データ漏えい事例から分かります。2018年5月、Honda Indiaでは、同社のモバイル車両管理・顧客サービスアプリHonda Connectのユーザーデータ5万人分が2つのパブリックAWS S3バケットで開示されるインシデントが発生しています。

2019年12月

26,000件

のホンダの北米顧客のPIIがElasticSearchデータベースを経由で誤って公開

2022年9月

296,000人

のトヨタ「T-Connect」の顧客が攻撃のリスクに5年間晒され続ける。

2019年7月

40GB

のホンダ内部ネットワーク情報が公開され

300,000人

のホンダの世界の従業員（CEO、CFO、CSOを含む）データが認証なしで閲覧可能に

自動車会社のパートナーのセキュリティ設定ミスが、企業機密の漏えいにつながる可能性もあります。関連ベンダーのセキュリティに関連するリスクに、自社の顧客を晒す危険性もあります。2018年に発生した事例では、カナダの産業オートメーションサービスプロバイダー、Level One Roboticsのサーバーの設定ミスにより、トヨタをはじめとする自動車メーカーの機密文書が公開されたことが明らかになりました。公開された157GBのデータには、組立ラインの回路図、工場の間取り図、ロボットの設計図や構成、VPNアクセスやIDバッジのリクエストフォーム、従業員のPII、会社の銀行関連情報などが含まれていました。大量のデータのバックアップを可能にするrsyncファイル転送プロトコルがどのサーバーに対してもファイル転送を可能にしていたため、rsyncポートにアクセスできるrsyncクライアントであればどこからでもデータがダウンロードできる状態となっていました。

2018年7月

157GB

の機密データが公開

サードパーティのリスク

上記のカナダでのインシデントのように、侵害は、複数の自動車メーカーにサービスを提供するベンダーをきっかけとして発生する可能性があります。例えば、Rapid7の研究者は、2021年5月に、犯罪フォーラムのユーザー「kurdishhacker」が、スズキやトヨタをなどの複数の国内自動車メーカーをサポートする組織が保有するサーバーへの、Webシェルアクセスを販売していることを観測しました。侵害されたサーバーは20件以上のウェブサイトをサポートしていました。この攻撃者は、サーバーに知られていないエクスプロイトが存在し、サーバー管理者がWebシェルを削除ても、Webシェルを再インストールできると主張しています（図5）。

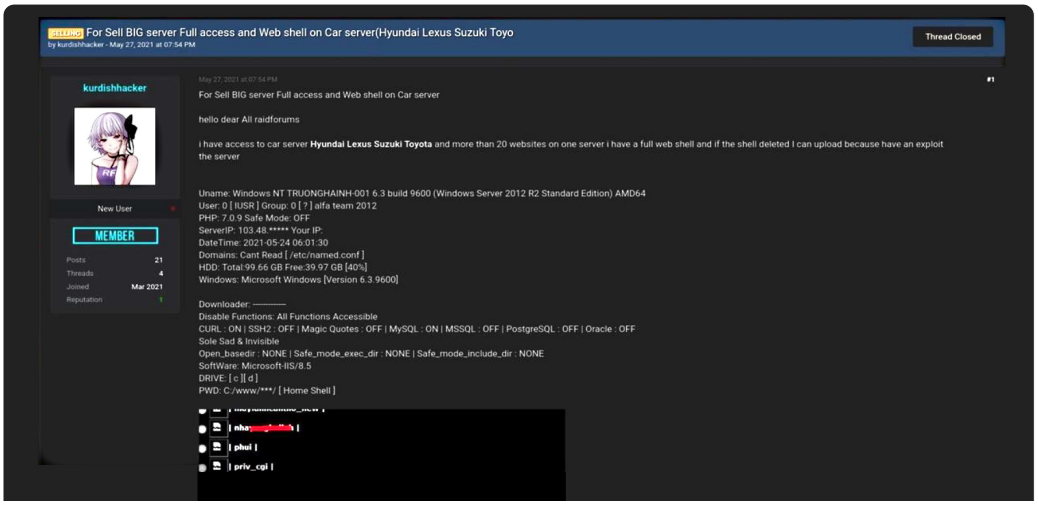
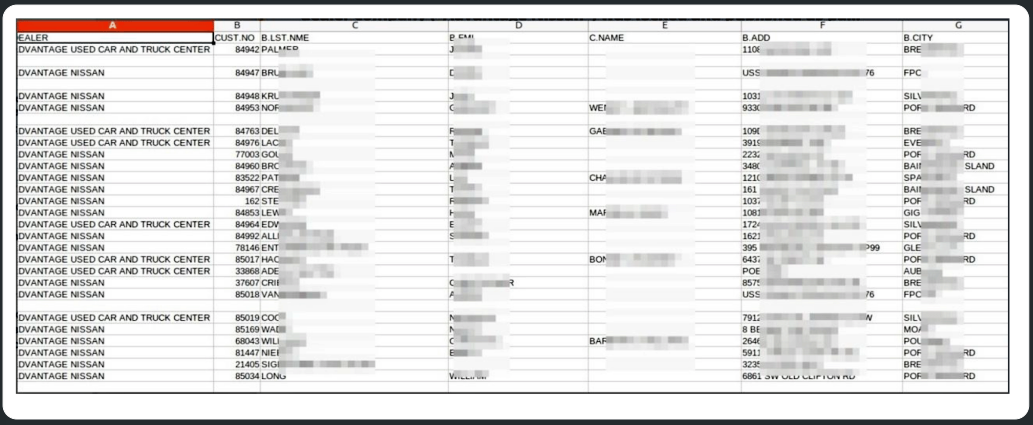


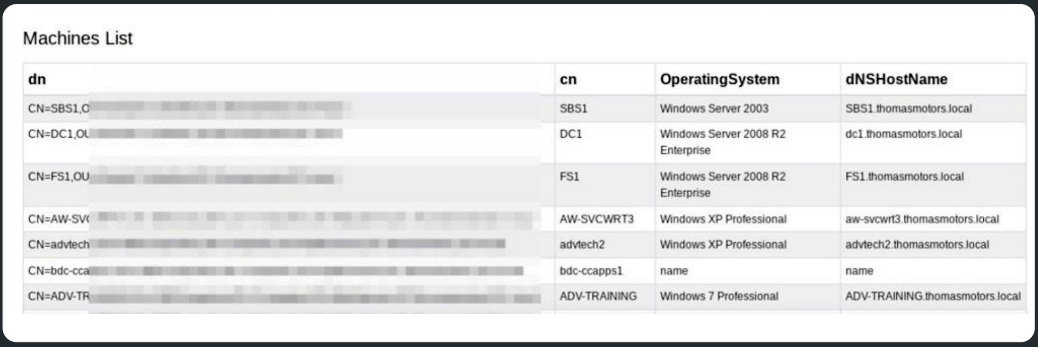
図5

正規販売店への侵害は、メーカーに影響を与える可能性があります。ランサムウェアによるデータ開示でディーラーデータが公開されると、販売・マーケティングなどの事業関連情報から競争力が低下したり、競合ブランドのメーカーやディーラーに競合情報が提供されるなどして、メーカーに影響が及ぶ可能性があります。加えて、その販売店が別会社であり、ブランド名を冠したメーカーが販売店のセキュリティを管理する立場になかったとしても、侵害を受けた販売店に関連するブランドへの消費者の信頼が失われる可能性があります。メーカーのディーラーポータルなど、販売店とメーカーに共有のインフラストラクチャへのアクセスがある場合、販売店での侵害の発生がメーカーへの攻撃につながる可能性もあります。例えば、2020年10月、Rapid7の研究者は、ランサムウェアオペレーターが米国の日産ディーラーを侵害することで取得したとする顧客データ、マシンのリスト、その他の機密データを開示したことを確認しています（図6および7）。



A	B	C	D	E	F	G
EALER	CUST.NO	B.LST.NME	B.EMI	C.NAME	B.ADD	B.CITY
DVANTAGE USED CAR AND TRUCK CENTER	84942	PALMER	J		1108	BRE
DVANTAGE NISSAN	84947	BRU	C		USS 76	FPC
DVANTAGE NISSAN	84948	KRU	J		1031	SILV
DVANTAGE NISSAN	84953	NOF	C	WEI	9330	POF RD
DVANTAGE USED CAR AND TRUCK CENTER	84763	DEL	F	GAE	1096	BRE
DVANTAGE USED CAR AND TRUCK CENTER	84976	LAC	T		3910	EVE
DVANTAGE NISSAN	77003	GOL	M		2232	POF RD
DVANTAGE NISSAN	84960	BRC	A		3480	BAI SLAND
DVANTAGE NISSAN	83522	PAT	L	CHA	1210	SPA
DVANTAGE NISSAN	84967	CRE	T		161	BAI SLAND
DVANTAGE NISSAN	162	STE	F		1037	POF RD
DVANTAGE NISSAN	84853	LEV	H	MAI	1081	GIG
DVANTAGE USED CAR AND TRUCK CENTER	84964	EDV	E		1724	SILV
DVANTAGE NISSAN	84992	ALL	S		1621	POF RD
DVANTAGE NISSAN	78146	ENT			395 099	GLE
DVANTAGE USED CAR AND TRUCK CENTER	85017	HAC	T	BON	6437	POF RD
DVANTAGE USED CAR AND TRUCK CENTER	33868	ADE			POE	AUB
DVANTAGE NISSAN	37607	CRI	C R		8575	BRE
DVANTAGE NISSAN	85018	VAN	A		USS 76	FPC
DVANTAGE USED CAR AND TRUCK CENTER	85019	COC	N		7912 W	SILV
DVANTAGE NISSAN	85169	WAL	N		8 BE	MOV
DVANTAGE NISSAN	68043	WIL	C	BAF	2646	POL
DVANTAGE NISSAN	81447	NEI	E		5911	POF RD
DVANTAGE NISSAN	21405	SIG			3235	BRE
DVANTAGE NISSAN	85034	LONG	WILL		6861 SW OLD CLIFTON RD	POF RD

図6



Machines List

dn	cn	OperatingSystem	dNSHostName
CN=SBS1,O	SBS1	Windows Server 2003	SBS1.thomasmotors.local
CN=DC1,OU	DC1	Windows Server 2008 R2 Enterprise	dc1.thomasmotors.local
CN=FS1,OU	FS1	Windows Server 2008 R2 Enterprise	FS1.thomasmotors.local
CN=AW-SV	AW-SVCWRT3	Windows XP Professional	aw-svcwrt3.thomasmotors.local
CN=advtech	advtech2	Windows XP Professional	advtech2.thomasmotors.local
CN=bdc-cca	bdc-ccapps1	name	name
CN=ADV-TR	ADV-TRAINING	Windows 7 Professional	ADV-TRAINING.thomasmotors.local

図7

ビジネスメール侵害

さまざまな業種および組織に影響を及ぼすビジネスメール詐欺（BEC）攻撃では、自動車関連企業も標的となりえます。BEC攻撃は、侵害された電子メールアカウントを使って役員やパートナー企業を装ったり、実在の人物になりすまして従業員を騙し、多額の金銭を攻撃者に送信させるものです。攻撃者は通常、スピアフィッシング攻撃やキーストロークロガーで正規のメールアカウントを侵害して入手したアクセス権を利用して、従業員に送金をそそのかしたり、業務プロセス情報をん入手して悪用しようとします。トヨタ車向けにシートや内装を供給している欧州の子会社は、2019年8月にBEC攻撃を受け、3,700万米ドルという多額の被害を被りました。これは、攻撃者が同社の従業員にソーシャルエンジニアリングを仕掛け、不正に改ざんされたベンダー請求書を送り、送金を促したものです。

2019年8月

370万米ドル

ビジネスメール詐欺（BEC）攻撃で発生した損失額

国内自動車業界で最も狙われているのは自動車本体のメーカーと言えますが、被害者はこれにとどまりません。例えば、2020年11月、犯罪フォーラムのユーザー「pizza50」は、侵害が報告されている、ある国内中古車輸出事業者のユーザーデータベースを250米ドルで販売すると申し出ています。データベースには、27,547人のユーザーのユーザー名、平文パスワード、メールアドレス、電話番号、生年月日、その他の情報が含まれていました。攻撃者は、SQLインジェクション（SQLi）攻撃でこのデータベースを侵害したと主張しています（図8）。

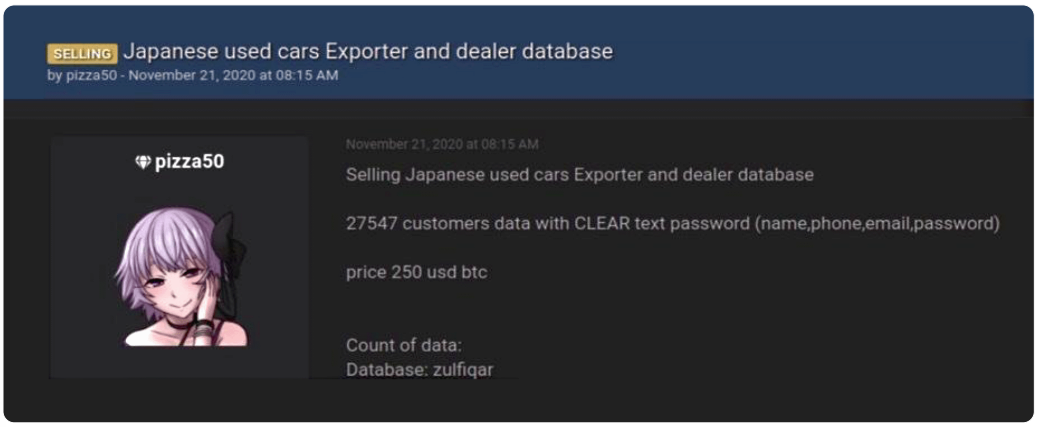


図8

金融サービス

世界中の金融機関は犯罪者が重点的に狙う標的となっていますが、日本も例外ではありません。日本の豊かな経済とそれを支える金融業界は、世界中の犯罪者にとって格好の標的となっています。

暗号通貨取引所

従来の金融機関のほか、暗号通貨取引所もサイバー攻撃の標的となっています。東京を拠点とする取引所Mt. Goxから約4億6000万米ドル相当の暗号通貨が盗まれた件は、この業界でも重大なインシデントとなり、2014年の発覚以降、暗号通貨取引所からさらに大規模な窃盗事件が続出しました。

最近では、2021年8月に日本の暗号通貨取引所Liquidが約9,700万米ドル相当の暗号通貨の盗難に見舞われました。コインチェック事件の場合と同様に、Liquidは被害に遭った暗号通貨を安全性の低い「ホットウォレット」に保管しており、この事件の発生後、より安全な「コールドウォレット」に移動しています。その他、日本企業に起こった多数の侵害と同様に、同社は、これらの盗難がシンガポール子会社、Quoineのマルチパーティ計算（MPC）ウォレットの侵害から始まったと判断しました。別件と思われる2020年11月のインシデントで、Liquidはホスティングプロバイダー経由のDNSハイジャック攻撃を受けており、この際、攻撃者は顧客の氏名、住所、メールアドレス、ハッシュ化されたパスワードに加え、さらに多くのPIIデータポイントの侵害に成功したものと考えられています。

顧客データの侵害

フィッシングは、日本を始め、世界中の金融機関の顧客の認証情報を狙う一般的な犯罪手口です。日本で2021年に発生したフィッシング攻撃を例に取ると、フィッシングページのなりすまし対象として最も多かったのは金融業で、全体の31%を占めていました。これらのフィッシングドメインの多くは、サブドメインに「card」など金融サービスに関係する英語の文字列と、標的となる金融機関のブランド名を使用していました。しかし中には、日本語の国際化ドメイン名（IDN）を使用したものもありました。

世界の金融セクターに対する犯罪活動に関する脅威インテリジェンス情報の多くは、ロシア語圏または英語圏の地下犯罪組織に起因するものですが、日本の金融セクターは中国語圏の犯罪者の標的にもなっています。例えば、Rapid7の研究者は、中国語を使用する犯罪フォーラムのユーザー「sherrybaby889」が、2020年10月に国内の銀行顧客48,201人分のデータベースを販売していることを観測しています。データベースには、氏名、電話番号、メールアドレス、住所、生年月日、認証情報などがわかるデータが含まれていました（図9）。

犯罪者は通常、オンラインバンキングの認証情報、小売業やサービス業界などへの侵害によって入手したカード情報を介して金融機関の顧客を狙います。日本の化粧品オンライン小売業者ACROの顧客10万人以上に影響を及ぼした支払いカード侵害の例でも分かるように、サードパーティである支払処理業者は、カードデータを一括で詐取する上で格好の標的となっています。攻撃者は、この支払処理業者のソフトウェアの脆弱性を悪用し、2020年5月から2021年8月の間に、ACROの2つの化粧品オンラインショップサイトから顧客のカード情報を収集しました。

図9

カード以外にも、オンライン決済サービス顧客の認証情報が標的となる可能性もあります。例えば、2022年11月には、あるAndroidマルウェアファミリーがオンライン決済プラットフォームの認証情報を侵害するため、日本国内ユーザーのデバイスを狙っていることが明らかになりました。SMS経由で日本語を使うこのソーシャルエンジニアリング攻撃は、セキュリティ上に問題があるように見せかけて被害者をそそのかし、マルウェアをインストールさせることを目的としていました。このマルウェアは、標的のサービスをエミュレートする偽の日本語プロンプトに決済サービスの認証情報を入力するようにユーザーに促し、侵害されたデバイスからリバースプロキシ接続を開始し、さらに攻撃者が被害者自身のIPアドレスから不正なトランザクションを開始できるようにして、正当な使用を装うことで、詐欺検出システムの検知逃れをしていました。

銀行自身が狙われることもあります。例えば、Rapid7の研究者は、犯罪フォーラムのユーザー名「WICK1」が、日本の銀行の侵害で取得したとする顧客データを販売していることを発見しています。

従業員データの侵害

金融機関に対する攻撃は、顧客の口座に関連する詐欺を狙ったものが一般的ですが、従業員を対象とする場合もあります。例えば、Rapid7の研究者は、犯罪フォーラムのユーザー「B14CK-J0K3R」が2020年11月に日本とオーストラリアの銀行員684,200人のPIIを販売したことを観測しています。このPIIデータベースには、IDとパスワード、住所、電話番号、メールアドレス、生年月日、母親の旧姓、国民識別番号、クレジットカード情報などがわかるデータが含まれていました（図10）。

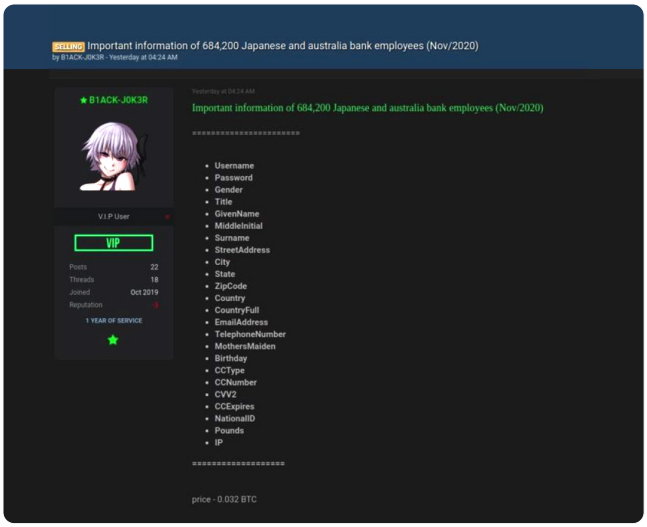


図10

テクノロジー、メディア、通信

テクノロジー企業は、企業自体をねらうのではなく、顧客情報やアクセスを求める攻撃者にとって価値のある標的です。情報技術（IT）ベンダーは、特にランサムウェアオペレーターの格好の標的です。例えば、マネージドサービスプロバイダー（MSP）などのITベンダーを踏み台にすれば、少ない労力で多数の企業に感染を広げられるためです。

2022年12月に発覚したあるITベンダーの侵害はまさにその好例でした。ランサムウェアによる大規模なサプライチェーン攻撃の発端となったこの侵害は、2023年初時点で、オンライン保険会社を始めとする10社以上の国内企業に影響を及ぼしています。同社は、攻撃者がその顧客を対象としたランサムウェア攻撃を仕掛けるために有用なデータを所有していたため、特にランサムウェア攻撃者にとって価値ある標的だったのです。

2020年5月の東京に本社を置くあるフォーチュン500企業の一社に対する侵害は、テクノロジー/通信会社の侵害が顧客のひとつであった政府に関する情報漏えいにつながった例であると同時に、国内のネットワークへの入口として日本企業の海外事業が悪用されることを示す例の一つでもあります。62の顧客組織に関する情報漏えいを招いた子会社のホスティング・クラウドサービスインフラストラクチャへの侵害は、シンガポールで同社の事業をサポートするマシンの侵害から始まったとされています。国内報道によると、この侵害により、防衛関連顧客に関する機密情報や通信インフラストラクチャが漏えいた可能性があるとのことです。

国内のテクノロジー、メディア、通信企業への攻撃の影響を受けているのは政府だけではありません。2022年5月、あるランサムウェア攻撃により、大規模なグローバル展開を行っている日本のメディア企業の、シンガポールを拠点とするアジア事業に影響が発生しました。同社の海外事業が標的となったのはこのインシデントが初めてではなく、2019年9月に、ニューヨークに勤務するある社員がBECの被害に遭い、同社役員を装った犯罪者に約2,900万米ドルを送金しています。

日本企業はゲーム市場でもリーダーの地位を占めています。そのため、攻撃者は消費者を狙う攻撃手法を用いて同業種を標的としています。例えば、2022年7月、BlackCat/AlphVランサムウェアグループが、パックマンやエルデンリングなどの有名なタイトルを発表している日本のゲーム会社を侵害したことが明らかになりました。BlackCatは、2021年5月に米国のコロニアルパイプラインを攻撃したDarkSideランサムウェアグループが名称変更したものとされています。同インシデントでは、攻撃者が同社のアジア事業のシステムに不正にアクセスしているため、同社はこの侵害でアジアの顧客に関するデータが危険に晒された可能性があるとしています。

まとめと提言

日本は世界第3位の経済大国であり、多くのグローバル企業やブランドの本拠地であるため、攻撃にさらされやすい状況となっています。自動車製造をはじめとする国内製造業は、日本経済にとって重要性が高く、また海外市場を率いる存在でもあるため、特に標的とされがちです。金融機関は通常、どこの国においても最大の標的ですが、日本の経済の豊かさから、日本国内の金融機関は、より、狙われる傾向にあります。国内のテクノロジー、メディア、通信企業は、侵害の影響範囲が官民両方の顧客や消費者に及ぶことから、頻繁に標的とされます。近隣諸国政府も、経済的、財政的、政治的な理由から、国内の官民両方の組織を標的としています。

以下は、日本国内の企業やその子会社が、攻撃に立ち向かうための推奨事項です。

- 従業員教育を徹底し、表記ミスや文法ミスなどの、日本語ネイティブではない人が書いたと思われる不自然なメールやインスタントメッセージに注意するようにしてください。不自然な日本語は、外国人攻撃者による、日本人をターゲットとしたソーシャルエンジニアリングでよくみかけられます。
- 拠点や子会社などの関連組織を海外に置く日本企業は、それらが踏み台となった侵害の影響で、国内本社のネットワークが水平展開などの被害を被らないようにする必要がありますが、具体的には以下の方法が考えられます。
    - 買収した企業から継承される可能性のあるリスクや既存の侵害を見極め、修正するために、M&Aプロセスに買収対象企業のセキュリティ評価を組み込む。
    - 海外子会社のセキュリティ慣行をより緊密に監視・調整し、本社のセキュリティベストプラクティスを確実に実装する。
    - 侵害された海外子会社への不正アクセスをきっかけに、攻撃者がを国内親会社のネットワークへ水平展開することを防ぐため、ネットワークセグメンテーションを採用する。

- サードパーティに対するリスクプログラムを確立し、万が一ベンダーやパートナーのデータやインフラストラクチャが公開された際にどのようなリスクが組織に発生するかを精査しておく。
  - セキュリティに関する考慮事項をベンダー選択プロセスに組み込む。
  - ベンダーやパートナーで発生したセキュリティインシデントの報告に関する要件を確立し、可能であれば契約書に盛り込む。
- 攻撃者が狙うデータは何かを見極め、ネットワークセグメンテーションやファイル暗号化などの方法で保護する。どんな情報が狙われるかを見極める際には、それらが悪用される可能性があるかどうかを考えます。
  - 顧客や従業員の個人情報が漏洩することによる、詐欺、あるいは金銭搾取目的での悪用。
  - データを公開するという脅迫は通常ファイル暗号化ランサムウェアと同時に発生するものですが、単独で発生する可能性もあります。
  - ビジネス上の競合、もしくは対立する国家に対する経済的、政治的あるいは軍事関連の情報が漏えいすることにより、相手を優位に立たせるような知的財産情報。
- ランサムウェアの恐喝には応じないこと。身代金の支払いは更なる攻撃につながります。支払いを行なった企業へのさらなる攻撃が発生することもあれば、他の企業を狙うきっかけにもつながります。攻撃者の軍資金の提供につながるほか、支払いに応じた企業は恐喝に弱いとみなされ、「カモリスト」に掲載されて犯罪グループ間で共有されることもあります。支払い以外の選択肢を取ることができなくなってしまった場合にのみ、支払いを検討するようにしてください。
  - ランサムウェアにおけるファイル暗号化への対抗策は、定期的かつセグメント化した上で、複数のバックアップを作成することです。こうすることで、万が一暗号化された場合にも支払いをせずにデータを取り戻すことができます。
  - あるいは、ネットワークセグメンテーションと事前の暗号化により、万が一ランサムウェア攻撃の被害に遭い、データが漏えいしても、開示のリスクと恐喝の影響を最小限にとどめることができます。
- 特に製造業は、ランサムウェアおよびICSを狙ったマルウェア攻撃に注意すべきです。攻撃はベンダーやサプライヤーなどで発生する可能性もあり、その場合、サプライチェーンが切れ、自社の製造プロセスに影響を及ぼす恐れがあります。「ジャストインタイム」製造を実践している製造業の場合、バックアップとなるサプライチェーンを事前に用意し、生産業務の中断を最小限に抑えるようにします。

セキュリティオペレーションに実務的観点を

Rapid7について

Rapid7は、デジタルトランスフォーメーションの加速に直面する組織のセキュリティプログラム強化の支援を通じ、あらゆる人にとってより安全なデジタルの未来を創造しています。最高レベルのRapid7のソリューションポートフォリオは、セキュリティ担当者がリスクを管理し、アプリからクラウド、従来のインフラストラクチャ、ダークウェブに至るまで、脅威のランドスケープ全体にわたって脅威を排除するための支援を提供します。Rapid7は、オープンソースコミュニティと最先端の研究を促進し、得られる洞察を製品の最適化に活用し、最新の攻撃方法に対応する力を世界のセキュリティコミュニティに届けます。世界中の11,000社以上のお客様組織に信頼され、業界をリードするソリューションとサービスで、企業が攻撃者の一歩先を行き、競争に先んじ、常に将来に備えるためのお手伝いをします。

RAPID7

製品

クラウドセキュリティ
XDR & SIEM
脅威インテリジェンス
脆弱性リスク管理
アプリケーションセキュリティ
オーケストレーションと自動化
マネージドサービス

ラピッドセブン・ジャパン株式会社
電話：03-6838-9720

詳細と無償評価版につきましては、https://www.rapid7.com/ja/try/insight/をご参照ください。