Deloitte.
デロイト トーマツ

Deloitte Cyber Trends & Intelligence Report

2020 Winter

Nov 2020
デロイト トーマツ サイバー合同会社
Cyber Intelligence Center (CIC)

はじめに

人・モノ・組織・社会インフラなどがあらゆる境界を越えてつながりあうデジタル時代に突入し、サイバーセキュリティは企業の重要な経営課題のひとつであると同時に、あらゆる経営変革に欠かせない要素となっています。

デロイトトーマツサイバー合同会社は、様々なクライアントの重要アジェンダに対して、サイバー戦略立案からオペレーションに至るまで一気通貫のサービスを提供しています。また、世界20カ国以上に拠点を構えているDeloitteのサイバー インテリジェンス センター(以下、CIC)を2016年5月に日本に開所して以来、Deloitteはセキュリティ監視サービス（TSM - スレット・セキュリティ・モニタリング）と個社および業界のサイバー脅威を収集・分析するインテリジェンスサービス(TIA - スレット・インテリジェンス・アナリシス）をクライアントに提供しています。センター開所から4年が経過し、CICのセキュリティ監視およびインテリジェンスサービスで得られた知見や観測された事実に対する分析を外部に定期的に発信することを目的として、本レポートを発行することといたしました。

本レポートではまず初めに、二重恐喝ランサムウェアを取り上げます。一時下火になっていたランサムウェアがより収益性の高い"二重恐喝"の手法を取り入れたことにより、二重恐喝ランサムウェアは標的とされた企業にとってより危険かつリスクの高い攻撃手法であるということをお伝えするとともに、海外子会社を含む日本企業での被害発生状況を報告いたします。

また2020年上半期は、Emotet(詳細p7)の対応に追われた企業が非常に多かったと思います。Emotetの拡散手法を改めて整理し、日本国内における業種別被害発生状況および使用されるメールの手法を分類し、その特徴を明らかにいたしました。

さらに、セキュリティ監視サービスでの観測事例として、パスワードリスト型攻撃の特徴と対処事例を合わせてご紹介し、最後に2017年からDeloitteが継続的に観察を続けているダークマーケットでのクレジットカード販売の概要と、スマホ決済アプリとの紐づけによる不正利用の可能性について言及いたします。

本レポートがデジタルトランスフォーメーションに関わる全ての企業、特にITセキュリティ部門のセキュリティ対策の参考として、また、CSIRT・SOCの業務に従事している方々の情報収集の一助としてご活用いただければ幸いです。

二重恐喝ランサムウェアの動向

二重恐喝ランサムウェアとは

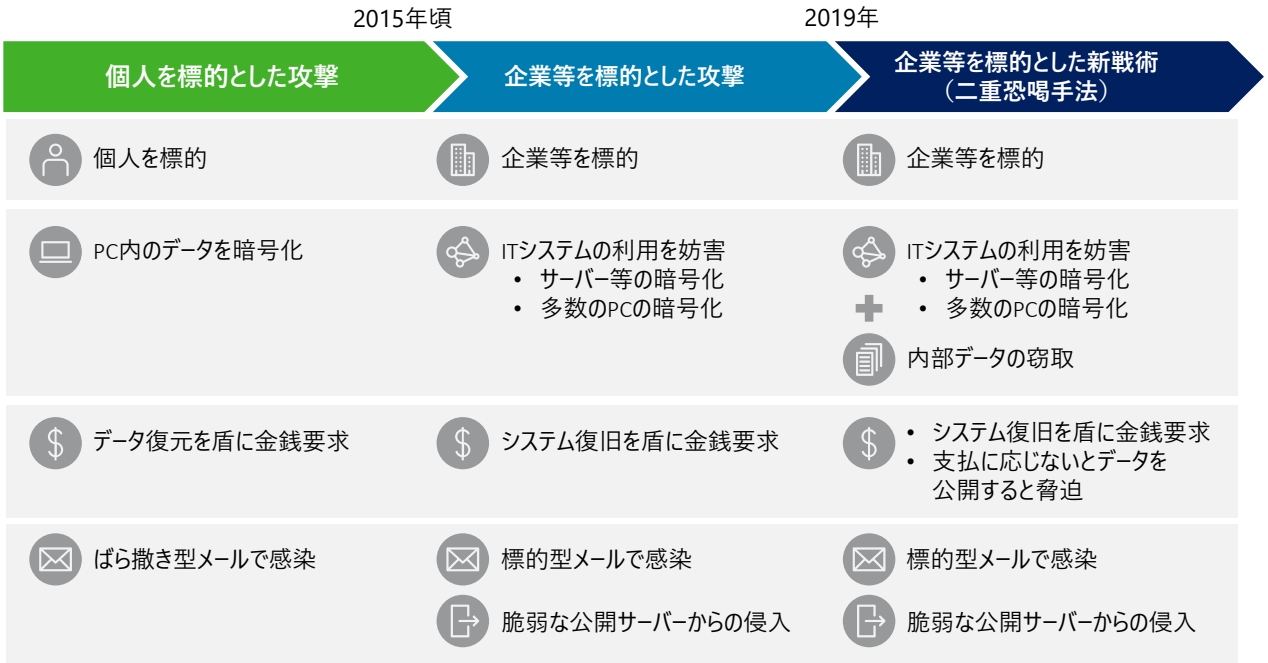
ランサムウェアはPCなどのデータを暗号化し、それを解除するためのカギと引き換えに金銭を要求するマルウェアです。

これまでは個人のPCを標的としていましたが、2015年頃から企業・団体を標的としたものが登場し、現在では企業・団体に対する主要なサイバー脅威のひとつとなっています。

2019年後半からは、新たに“二重恐喝 (Double Extortion)” と呼ばれる手法が流行し始めました。二重恐喝ランサムウェアが従来のランサムウェアと異なる点は、内部ネットワークに侵入して暗号化を行う前にデータを窃取するということで、暗号を解除するための支払いに応じなければデータを公開すると脅します。こうした従来の“データ復旧を盾にした恐喝”に加え、“データ公開を盾にした恐喝”を行うことから“二重恐喝”と呼ばれています。

ある二重恐喝ランサムウェアの攻撃者は、「GDPRで巨額の制裁金を課されるよりは、我々に支払った方がはるかに安いだろう」とアンダーグラウンドフォーラムで述べており、個人情報流出に対する企業へのペナルティを利用しようとしているものと見られます。

図表1　ランサムウェア攻撃のトレンドの変化

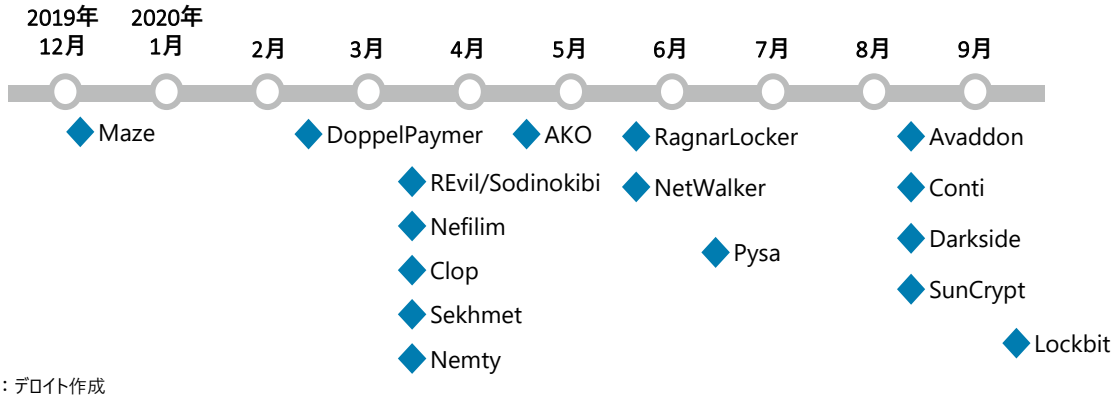


出所：デロイト作成

二重恐喝ランサムウェアによるデータ公開

二重恐喝ランサムウェアの攻撃者はダークWeb上に窃取データを公開するためのリークサイトを開設しており、支払いに応じない企業のデータを徐々に公開していくという戦術をとっています。多くのランサムウェア攻撃者がこの新たな戦術を取り入れており、リークサイトは非常に速いペースで増加しています。

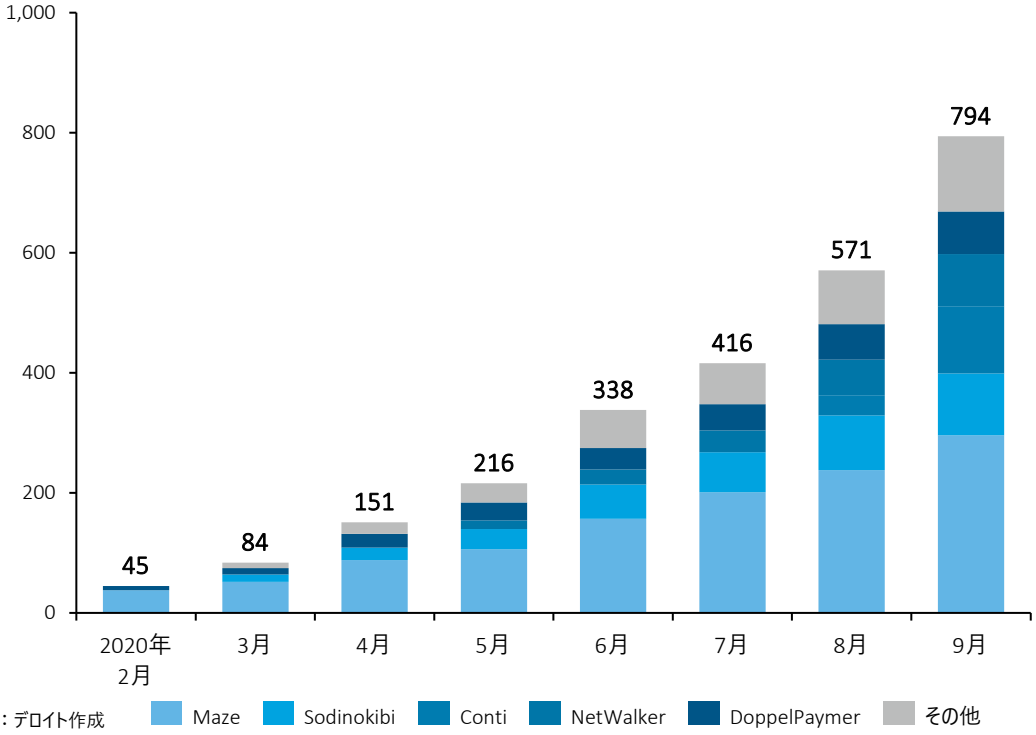
図表2　二重恐喝ランサムウェアリークサイトの開設時期



出所：デロイト作成

二重恐喝手法を取り入れたランサムウェアが次々と登場していることから、ランサムウェアのリークサイト上に公開された企業等の累計件数も月を追うごとに著しいペースで増加しています。

図表3　ランサムウェアのリークサイトでデータ公開された企業等の累計件数の推移



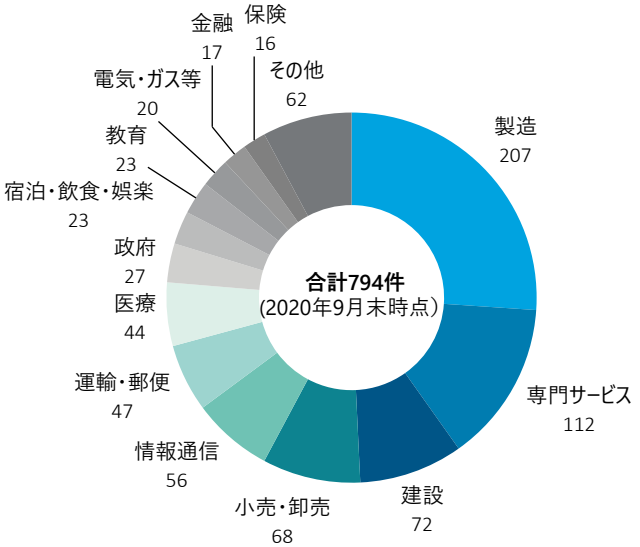
出所：デロイト作成
脚注：Maze、Sodinokibi等は二重恐喝ランサムウェアの名称

リークサイト掲載企業から見る被害の傾向

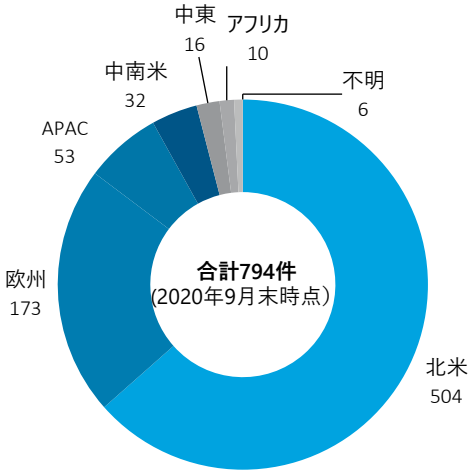
リークサイトに掲載された企業の業種別件数を見ると、製造業が圧倒的に多い結果となっています(図表4)。中小企業を含めるとセキュリティが甘く外部から侵入しやすい事業者が多いことや、ラインの停止が損失に直接結びつくためだと推測できます。製造業の中でも特に医療や重要インフラ分野は人々の命やライフラインに直結しているため大きな脅威となります。近年のサイバー脅威の拡大を受けて、2020年4月には国際刑事警察機構がCOVID-19緊急対応に関与する世界中の病院を標的にしたランサムウェアによるサイバー攻撃が急増しているとして、各加盟国の警察当局に通知を出しています(詳細は海外サイバーセキュリティニュース第106号をご確認ください)。また重要インフラ分野でも米国を中心にガイドラインの公表やサイバー訓練を行う等、業界ごとに対策を呼び掛けています。この他海外における具体的な事例、COVID-19に関連したロックダウン時のインシデント対応や重要インフラに関するDeloitteの考察はリンク内をご参照ください。

地域別で見ると北米が圧倒的に多く、次に欧州と続きますが、これらの地域は経済規模が大きく、多額の身代金の支払いが期待できるほか、支払いに応じるケースが多いためだと考えられます。欧米地域ではサイバー保険によるカバー、交渉や支払いを代行するインシデント対応事業者の存在など被害発生時の対応態勢が整っていることから、金銭による解決が行いやすくなっているがために、却って狙われやすくなっているという可能性があります。

図表4　リークサイトに公開された業種別企業件数



図表5　リークサイトに公開された地域別企業件数



出所：図表4、5共にデロイト作成

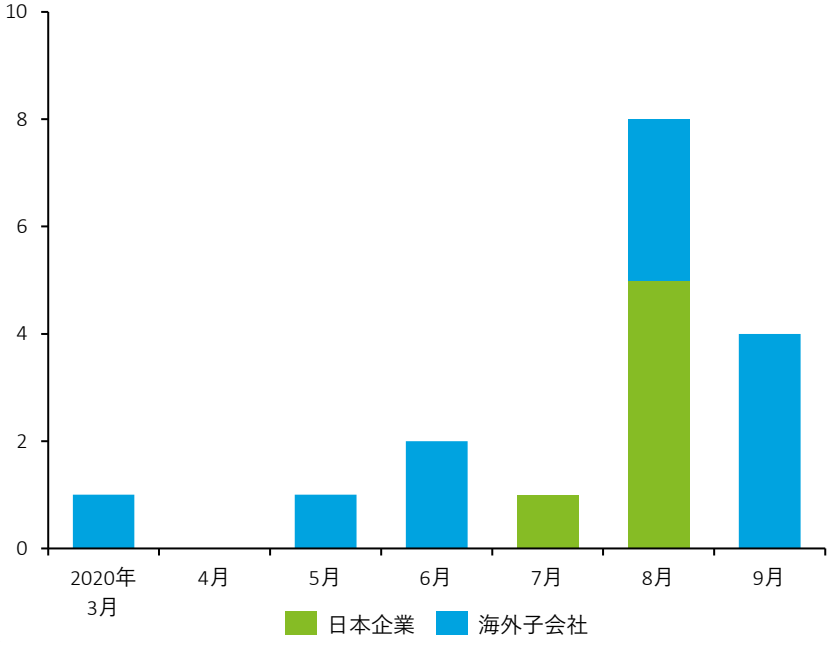
二重恐喝ランサムウェアと日本

2020年5月以降、海外子会社を含めた日本企業のデータは公開され続けています。特に8月には5件の日本企業・団体のデータが公開されており、その被害は徐々に増えてきていることから、対岸の火事ではないということは明らかです。

二重恐喝ランサムウェアでは、不用意に外部公開されたリモートデスクトップ接続サービスや脆弱なVPNサーバーなどから侵入されるパターンが多く見られます。COVID-19によりテレワークが増加し、強制的に移行せざるを得ない企業も多かったと思いますが、十分な準備がないまま導入されたVPNサーバー等は、攻撃者から見れば格好の獲物になるのです。

脆弱な状態のサーバーを公開するということは、今や企業の事業継続全体に関わるリスクといえます。攻撃者は常に脆弱なサーバーがないか探し回っているため、定期的に自社に弱点がないか能動的にチェックし、発見された弱点を修正するサイクルを回すことが重要です。

図表6　リークサイトに公開された海外子会社を含む日本企業の件数



出所：デロイト作成

日本におけるマルウェア“Emotet ”の被害拡大

2020年7月から、日本を含む世界中でマルウェア “Emotet ”の拡散キャンペーンが再開されました。取引相手とのやりとりに見せかけたメールを送るという、2019年から確認されている拡散手法から大きな変更はありませんが、これに加えてパスワード付きzipファイルが添付されるという手口が使われた攻撃が2020年9月以降に確認されるなど、より巧妙さを増しています。

Emotetの概要

Emotetは2014年頃に初めて確認されたマルウェアで、元々はPC内に保存されたオンラインバンキングなどの情報窃取を目的としたバンキングマルウェアでした。2016年頃からは機能を転換し、“ローダー“として使用されています。ローダーは別のマルウェアをダウンロードしてインストールするためのマルウェアで、Emotetの背後にいる攻撃者は、同マルウェアを使用したマルウェアの配布代行サービスで利益を得ているものと考えられます。

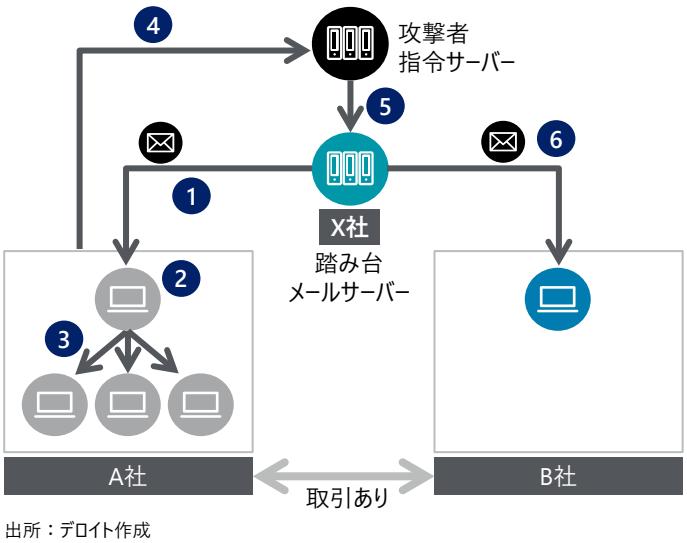
2019年9月に世界中で大規模なメールによる拡散キャンペーンが行われ、同年10月からは日本に対する攻撃も活発化、複数の企業・団体で感染被害が発生しました。この拡散キャンペーンは2020年1月に収束し、しばらくは活動が見られませんでしたが、2020年7月以降再び日本を含む世界中で拡散キャンペーンが開始されています。

Emotetの拡散手法

2019年以降のEmotet拡散キャンペーンで注目されるのは、その攻撃メールの巧妙さです。感染PCから窃取したメールの本文やアドレス帳をもとに、感染PCとメールのやりとりがあった相手に対して、その続きを装った攻撃メールを送ることで受信者が不正ファイルを開く可能性を高めています。

図表7はEmotetによる拡散の流れを示したものです。図表内の⑥でPCの感染に成功した場合、感染PC内のメール情報を使用して別会社に不正メールを送り、感染を拡大していきます。主に不正なマクロが仕込まれたWordファイルが使用されており、受信者がファイルを開き、“マクロの有効化”や“コンテンツの有効化”を許可してしまうとEmotetに感染するという手口が使われます。

図表7　Emotet拡散の仕組みと流れ



①	A社の取引先を装った不正メール送信 (不正なWordファイル添付)
②	• ファイルを開いてしまい、Emotetに感染 • PC内に保存された認証情報の窃取 • メール情報の窃取
③	窃取した認証情報を使用し内部ネットワークで感染拡大
④	窃取した情報を攻撃者の元に送信
⑤	A社から窃取したメール情報をもとに、B社宛の不正メールを作成
⑥	A社・B社間のメールのやりとりの続きを装った不正メール送信

出所：デロイト作成

メールの件名・添付ファイル

日本の拡散キャンペーンにおいて、メールの種類は概ね6種類に分類できます。またこれにより、Emotetの攻撃メールには次の特徴があります。

- "なりすまし"パターンでは、単なる英数字のみの名前のファイル、または変更、修正等の文言が含まれるファイルが添付されることが多い
- その他のパターンでは、件名と添付ファイル名がほぼ同じであることが多い
- 添付ファイルは、ほとんどの場合不正なマクロが仕込まれたdocファイルである

図表8　日本での主なEmotet拡散メール

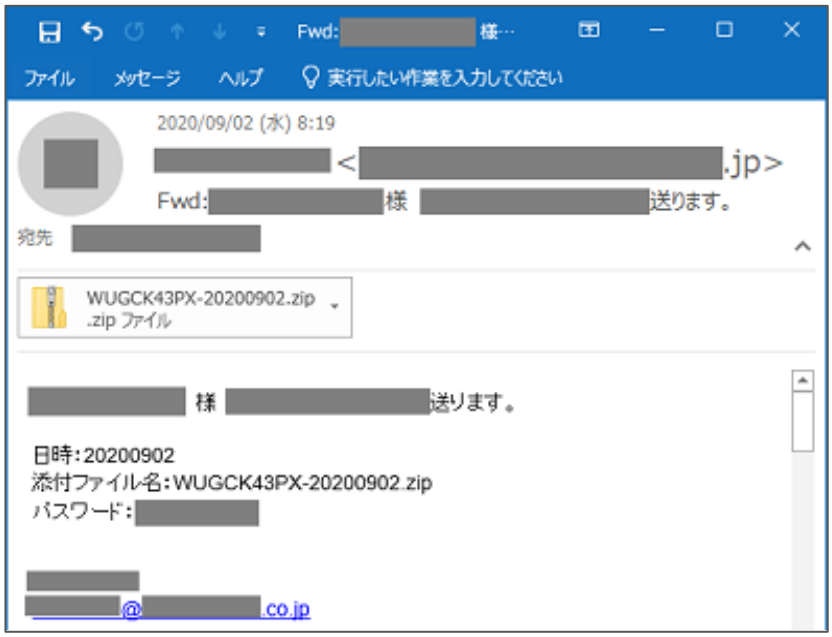
メールの種類	件名例	添付ファイル例
なりすまし	• Re: [実際にやりとりされていた件名] • Re: [宛先表示名] • Fwd: [宛先表示名]	• [英数字十数桁].doc • [英数字十数桁].zip • 変化[日付].doc • からの変更[日付].doc
請求書	• ご入金額の通知・ご請求書発行のお願い [数字記号日付] • 請求書送付のお願い [数字記号日付] • 請求書ステータスの更新 • 支払請求書 • 未請求書	• ご入金額の通知・ご請求書発行のお願い [数字日付].doc • [英数字] 請求書送付のお願い.doc • [英数字] 請求書の件です。.doc
会議	• ビジネス会議への招待 [ドメイン名] • 会議への招待 [ドメイン名] • ミーティング [ドメイン名]	• ビジネス会議への招待.doc • 会議への招待.doc • ミーティング.doc
新型コロナ	• XXXX保健所福祉室 [日付]*1	• XXXX保健所福祉室 [日付].doc*1
アンケート	• XXX社・カスタマー満足度アンケート調査ご協力のお願い*1 • XXX社・サポートセンター満足度アンケート調査　ご協力のお願い*1	• XXX社・カスタマー満足度アンケート調査ご協力のお願い.doc *1 • XXX社・サポートセンター満足度アンケート調査ご協力のお願い.doc *1
その他	• 通知 [日付] • 別添 [日付] • 消防検査 • 助けてください	• 通知 [日付].doc • 別添 [日付].doc • 消防検査.doc

出所：デロイト作成

*1　実際のメールにはそれぞれ実在する保健所名、セキュリティ企業名が記載されている

2020年9月以降には実在するセキュリティ企業のアンケートを騙ったメールが新たに確認されていることから、攻撃者が攻撃メールを継続的に改良していることがうかがえます。また、同じく9月以降にパスワード付zipファイルが添付された攻撃メールも確認されています。このzipファイルには不正なマクロが仕込まれたdocファイルが格納されており、docファイルを開いてマクロを有効にするとEmotetに感染してしまいます。

図表9　パスワード付zipファイルが添付された攻撃メールの例



出所：IPA,「Emotet」と呼ばれるウイルスへの感染を狙うメールについて

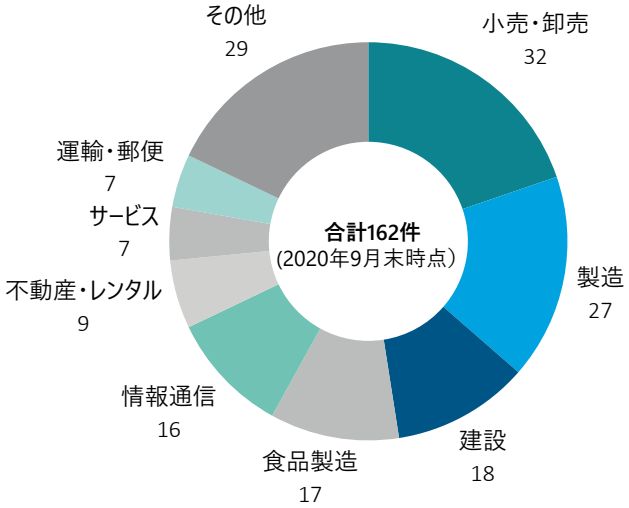
添付ファイルをパスワード付zipファイルで送るという方法は、日本でよく見られる習慣です。本手法は日本におけるメール習慣を悪用したものであり、かつ、添付ファイルの検査も無効化される可能性が高いため十分な注意が必要です。

日本における被害発生状況

図表10は、Emotetの被害にあったと推測される日本国内の企業・団体の業種別件数です。Deloitteは次のいずれかに該当する企業・団体等をEmotetによる被害を受けたとして集計しています。

- Emotetの被害にあったと公表した
- マルウェア被害にあったと公表し、その公表内容からEmotetの可能性が高いとDeloitteが判断した
- Emotetの攻撃メールの送信元として観測されたメールアドレスを所有する企業・団体

図表10　日本における業種別Emotet被害件数



出所：デロイト作成

Emotetは日本だけでなく海外でも同様に被害が拡大しており、2019年11月には米国マルウェアバイトが医療分野のマルウェア脅威報告書を公表しました。医療業界でもマルウェア脅威としては、EmotetやTrickBot等が目立っています (詳細は海外サイバーセキュリティニュース第98号をご確認ください)。

パスワードリスト型攻撃の動向

パスワードリスト型攻撃は、あるサイトから流出したメールアドレス・パスワードのセットを用いて他のサービスへの不正ログインを試みる攻撃で、複数のサイトで同じID、パスワードを使い回しているユーザーが被害を受けます。ダークWebのフォーラム等ではパスワードリスト型攻撃に利用可能な流出データが出回っており、脅威実行者はこれらを利用することで容易に攻撃を実行することができます。DeloitteはダークWebから無料で入手可能な流出データを継続的に収集していますが、日本のメールアドレス・パスワードのセットは1億2,000万件を超える数となっています。

パスワードリスト型攻撃自体は目新しい手法ではないものの、2020年8月以降複数の企業で被害が報じられています。

図表11　2020年8月以降に発生した企業向けパスワードリスト型攻撃

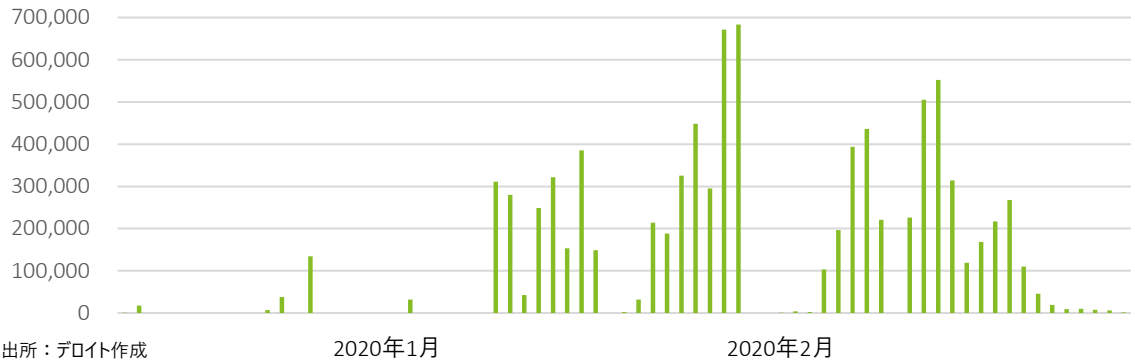
公表日	攻撃被害企業業種	攻撃期間	不正ログイン件数	金銭的被害等
8月5日	小売	5月5日～8月3日	約53,000件	なし
8月6日	運輸・インフラ	8月5日	5件	なし
8月11日	運輸・インフラ他	7月24日～8月2日	1,094件	ポイント交換被害
8月28日	ITサービス	8月19日～8月24日	337件	なし
9月12日	ITサービス	7月～9月	73,978件	なし
9月16日	金融	未公表	6件	不正出金
9月18日	金融	9月14日～9月17日	209件	なし
9月23日	運輸・インフラ	9月13日～9月15日	1,269件	ポイント交換被害
9月24日	情報通信	9月23日以降継続的	約800件	なし

出所：各種公開情報をもとにデロイト作成

パスワードリスト型攻撃の分析と特徴

Deloitte CICのセキュリティ監視サービス（以下、CIC監視）では、セキュリティ機器だけでなくWebサーバーやWebアプリケーションの監視もスコープとしており、パスワードリスト型攻撃の検知およびWAF等と連携した遮断を行っています。ここでは、実際に行われたパスワードリスト型攻撃の分析結果から見えてきた攻撃の特徴を解説します。

図表12　パスワード型攻撃のログイン試行回数例



出所：デロイト作成

攻撃に先んじた偵察フェーズ

今回ご紹介するケースでは、単位時間内に同一IPアドレスから複数IPアドレスを使ったログイン試行のしきい値を超えた攻撃を2020年初頭に検知しました。その後の分析により、しきい値を超えない範囲での偵察活動がその1ヶ月ほど前から行われていたことが判明しました。この偵察フェーズでは、Webサイトで許可されているブラウザの言語設定や、CIC監視のしきい値や、ユーザーエージェント等の監視パラメーターを確認すると同時に、Webサイト全体の構成を把握することを目的としていたことが浮かび上がってきました。

ユーザーエージェント・言語設定の変更

当該Webサイトへの攻撃は2019年にも発生しており、その際に使われたユーザーエージェントが特徴的だったことから、それを監視パラメーターとして使用し、WAFによる遮断を行っていました。

しかしながら、2020年初頭の数か月後に行われた第2波の攻撃では、ユーザーエージェント情報が若干古いものの次に示すような一般的なものに変更されていたため、ユーザーエージェント単体で監視パラメーターとして活用することは難しい状況となっていました。

図表13　2019年の攻撃に使用されたユーザーエージェント情報

Mozilla/5.0 (Linux; Android 5.1.1; xxxxx Build/LMY48Z) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/39.0.0.0 Mobile Safari/537.36 CLIENTxxx/xxx	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:64.0) Gecko/20100101 Firefox/64.0

出所：デロイト作成
脚注：赤字は任意の文字列、黄緑はスマートフォンのモデル名を示す

また、2019年の攻撃ではブラウザの言語設定(Accept-Language)が中国語または英語に設定されていたことから、監視パラメーターとして有効でしたが、2020年に入ってからの攻撃では、日本国内のユーザーが使用するブラウザの設定としては一般的な日本語または英語設定に変更されており、有効な監視パラメーターではなくなっていました。

図表14　2019年の攻撃に使用された言語設定(Accept-Language)情報

zh-CN,en-US;q=0.8

図表15　2020年の攻撃に使用された言語設定(Accept-Language)情報

ja,en-US;q=0.7,en;q=0.3

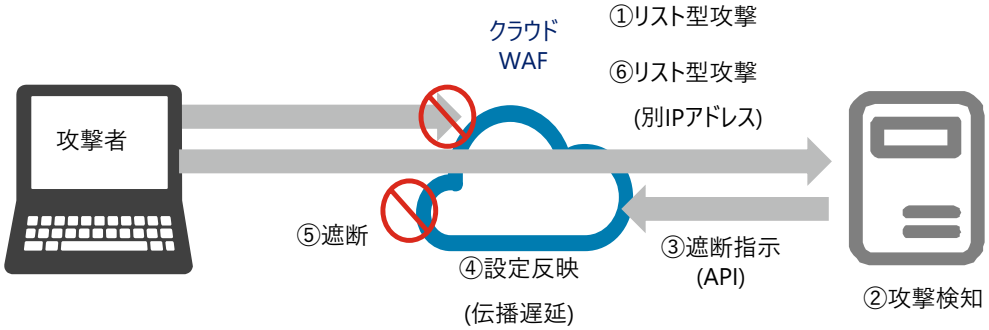
出所：デロイト作成

1IPアドレス当たりの攻撃間隔

2020年初頭のパスワードリスト型攻撃に対し、早期終息を最優先とすることをクライアントと合意した後、クラウドWAFのAPI経由で検知したIPアドレスの自動遮断を開始しました。それによって攻撃の効率が低下し、金銭的メリットが少なくなったことから攻撃は短期間で終息しました。このことからも攻撃者は攻撃の効率を重要視していることが見て取れます。

その数か月後の第2波では、同一Webサイトに対する同一の攻撃者からと思われる（ユーザーエージェント等から判断）パスワードリスト型攻撃を検知しました。前回の攻撃では、自動遮断を開始するまで比較的長期にわたりましたが、第2波の攻撃は2日間という短期間に集約されており、攻撃の内容もDeloitte CICによる監視・遮断能力を見定める"威力偵察"的な内容となっていました。

図表16　監視サービスにおける検知・遮断のシステム概要



出所：デロイト作成

以前の攻撃と明らかに異なっていた点は使用されるIPアドレス数および1IPアドレス当たりの攻撃間隔です。具体的には、2020年初頭の攻撃の際は1～4個の IPアドレスからログイン試行を25分から2時間45分程度行っていたのに対して、その数か月後の第2波の攻撃では2日間で1,150個ほどのIPアドレスが用いられ、1IPアドレス当たりの攻撃時間(図表16の①から⑥の時間間隔)が1分以内と非常に短くなっていました。また、1IPアドレス当たりのログイン試行回数が両日共に約10回であったことから、1つのIPアドレスから10回のログインを試行し、1分後には別のIPアドレスから攻撃を繰り返す動作がプログラムされていることが伺えます。

図表17　2020年第2波のパスワードリスト型攻撃概要

攻撃発生日	IPアドレス数	ログイン試行回数	1IPアドレス当たりの攻撃時間(①-⑥)
1日目	211	2,224	約60秒
2日目	936	9,358	

出所：デロイト作成

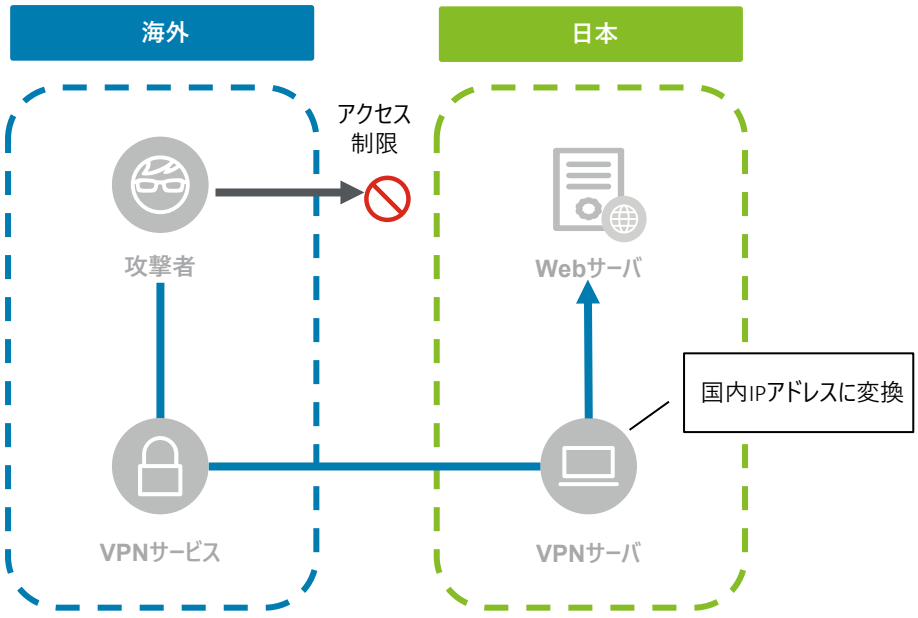
これは、2020年初頭の攻撃時に早期終息を最優先としたIPアドレス毎の自動遮断を開始したことに呼応し、1IPアドレス当たりの攻撃間隔を短くすることで、どの程度の間隔であれば自動遮断をかいくぐれるかを調査しながら攻撃を仕掛けていたと分析しています。

図表16の②から③は数秒で検知から遮断指示が発行されるため、1分程度の攻撃間隔であれば十分に遮断の効果が期待出来たものの、一部のクラウドWAFはサービスの仕様およびクラウドWAFシステムの負荷によって、遮断設定が全体に反映されるまでの時間（伝播遅延/プロパゲーションディレイ）が攻撃間隔である1分以上必要であることから、1分間隔でIPアドレスを変化させてくるパスワードリスト型攻撃を即時遮断するには至りませんでした。

一方で、攻撃者が用意しているBoTやProxyサービス、VPNサービスは限りある資源であり、数多くのIPアドレスを準備することは攻撃コストの増大につながります。第2波の攻撃で用意した約1,150のIPアドレスも、一度攻撃に使用すると次回攻撃時には遮断対象となることから、攻撃者の攻撃意欲を低減させることに成功したと言えるでしょう。

また、第2波の攻撃では北米の事業者が提供するVPNサービスで利用されているIPアドレスからの攻撃を多く検知しました。攻撃者はGeo IPと呼ばれる地域特定および特定の地域からのアクセス遮断を回避するためにVPNサービスを悪用したと考えられます。

図表18　VPNサービスを利用したGeo IPの回避手法



出所：デロイト作成

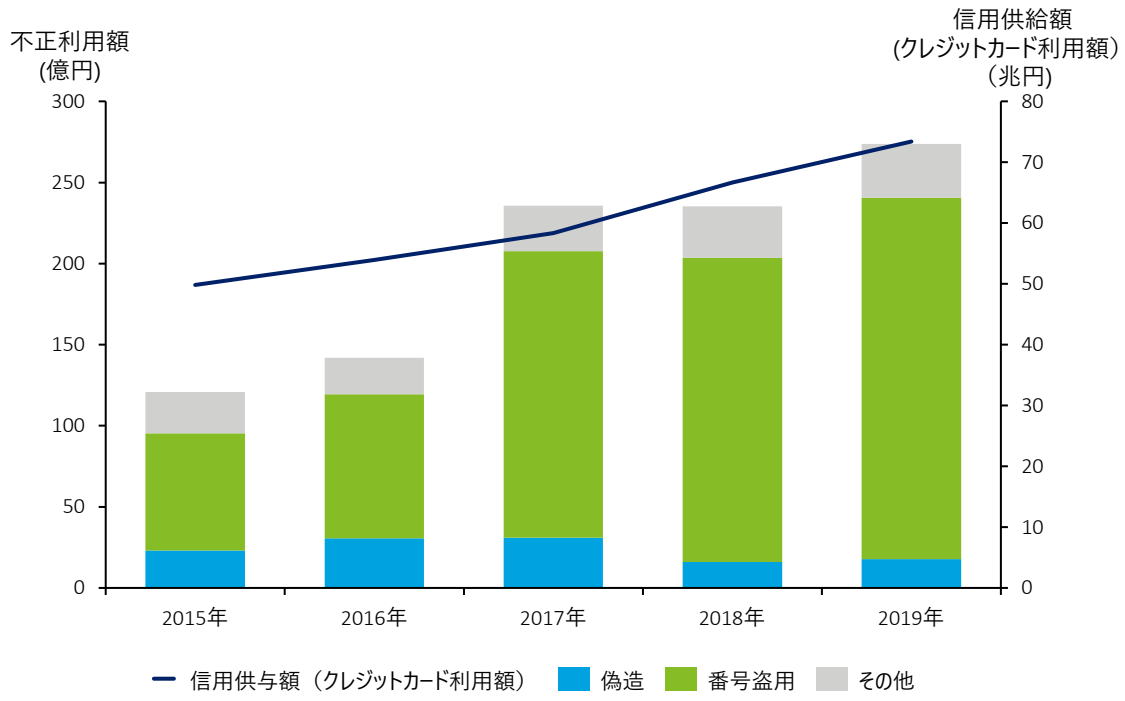
こういったVPNサービスが利用するIPアドレスのレンジ(/24単位)で遮断設定を投入することにより、より短時間で効率的な攻撃遮断を行うことが出来るため、Proxy、VPN事業者が提供するIPアドレスレンジのリストを準備することも有効な対策となり得ます。OSINTで得られる情報に加えて、こういったリストを提供するサービスもいくつかあるので、サービスの購読を検討することも選択肢のひとつであると考えます。

また、上述のようにIPアドレスレンジで遮断する場合には、正常通信を遮断する可能性も少なからずあります。ステークホルダー間で、誰がどういった条件で判断し、どのようなフローで連絡するかを事前に取り決めておくことも非常に重要です。

クレジットカード不正とダークWeb

日本国内におけるクレジットカード利用額は、2019年には約73兆円に達し増加の一途を辿っています。
一方、不正利用額も増加傾向にあり、2017年には年間200億円を超える規模になりました。不正利用のうち被害額が最も大きい"番号盗用"は、クレジットカード番号、名義人、セキュリティコードなどの情報が不正に取得され、オンライン決済に悪用される手口ですが、こうした情報は"CVV"と呼ばれ、ダークWebのマーケットで売買されています。

図表19　日本におけるクレジットカード利用額と不正利用額

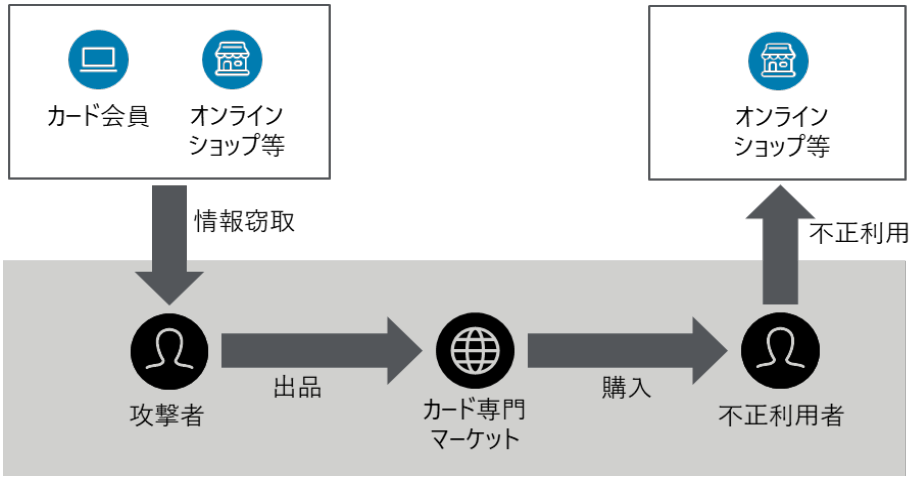


出所：一般社団法人日本クレジット協会の資料をもとにデロイト作成

カード専門マーケット

ダークWebにはクレジットカード情報の販売を専門とするマーケットが複数存在しており、犯罪ビジネスとして成立しています。クレジットカード情報の窃取とクレジットカード情報の不正利用では必要となるスキルがまったく異なりますが、こうしたマーケットが存在することでサイバー犯罪者はそれぞれの得意分野で不正な利益を得ることができるのです。

図表20　カード専用マーケットを活用した犯罪ビジネス



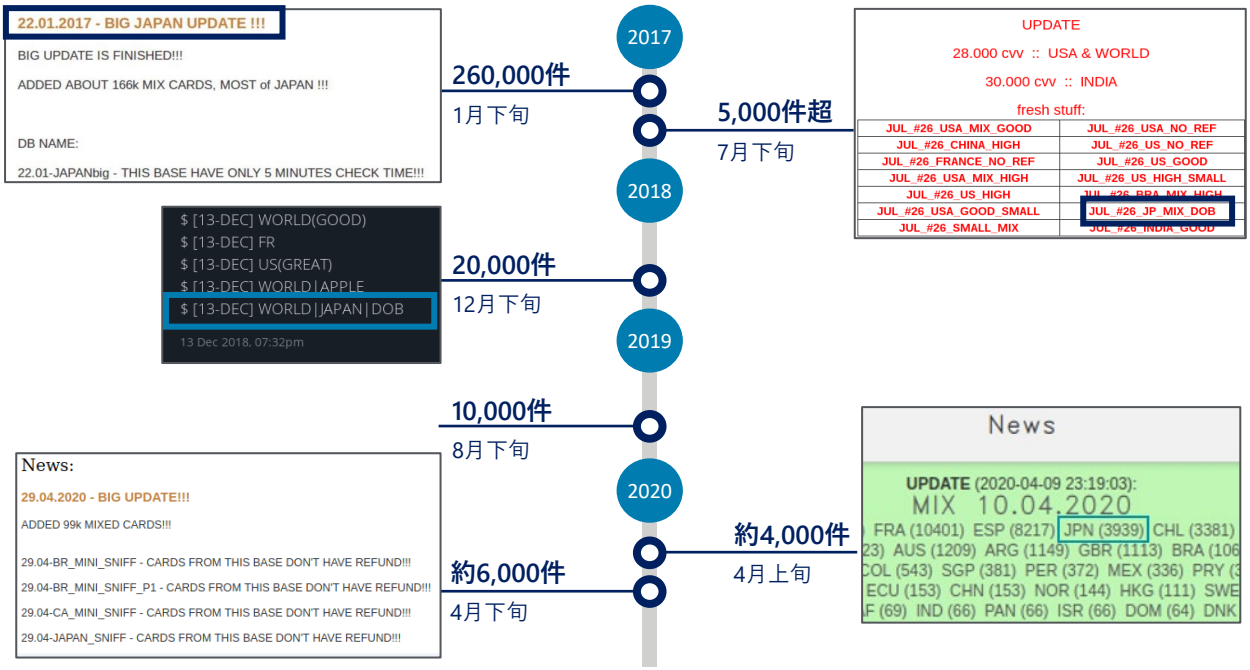
出所：デロイト作成

カード専門マーケットで販売されている情報のなかには、カード番号やセキュリティコードはもちろん、3Dセキュアのパスワードや所有者氏名、生年月日、住所など完全に他人になりすますための情報も“FULLZ”として販売されています。クレジットカード会社は本人確認の強化といったセキュリティ強化を進めているものの、攻撃者もそうした対策をさらに突破し必要情報を入手するための手口を洗練させているため、不正利用を完全に防ぐことは困難です。

ダークマーケットと日本のクレジットカード情報

ダークマーケットで売買されるクレジットカード情報のなかには、日本のカード会社が発行した情報も含まれています。Deloitteは2017年からダークマーケットのモニタリングを行っていますが、日々新たな日本のクレジットカード情報の出品を確認しています。一度に大量のクレジットカード情報が出品された事例も複数確認しており、2017年に発生した約26万件の大量出品をはじめ、毎年数千～数万件規模の出品が観測されています。

図表21　ダークマーケットで売買されたクレジットカード情報件数



出所：デロイト作成
脚注：1度に4,000件以上出品されたケースのみを記載

決済サービスとクレジットカード不正

日本でも、QRコード決済サービスに代表されるような、金融機関以外が提供する決済手段の普及が進んできています。こうした新たな決済手段の登場は利便性の向上につながる一方で、サイバー犯罪者にとっても悪用のチャンスとなり得ます。不正利用の観点から見ると、利用者と金融機関以外の外部決済事業者が介在することによって、次のような隙が生じやすくなります。

- 他人のクレジットカード情報や銀行口座などへの不正な紐づけ
  - クレジットカード情報などを連携させる際の本人確認が不十分な場合、なりすましによって不正に紐づけされる恐れがある
- 不正利用の容易性
  - 外部決済サービス経由で利用された場合、金融機関による不正利用の検知が困難となる
  - 決済アプリを利用して実店舗で決済された場合、不正利用の痕跡が残らず不正利用者の特定が困難となる

クレジットカード情報や銀行口座との不正な紐づけによる被害はたびたび発生しており、米国では医療費関連オンラインアプリケーションに不正アクセスがあり、地域医療機関向けの退役軍人医療費支払分が転用されたインシデントも発生しています(詳細は海外サイバーセキュリティニュース第116号をご確認ください)。

こうした被害は決済サービスの普及に対する大きな課題であり、前述のようなクレジットカード情報の売買の実態や、パスワードリスト型攻撃による個人情報の流出を考えれば、本人認証においてよく流通している情報のみを用いることはリスクとなります。

サイバー犯罪者の活動を理解し、利用者のどういった情報が流通しているかを把握することは、安全なサービス設計を行ううえで重要です。

おわりに

本レポートでは、二重恐喝ランサムウェアの動向、マルウェアEmotetの特徴、パスワードリスト型攻撃の動向、クレジットカード不正とダークWeb、と4つのテーマを取り上げました。EmotetについてはCIC監視において複数の企業で観測されています。リモートワークの増加に伴い、各社既存の通信経路での対策ではなく、エンドポイントでの対策強化が急務となっています。

本レポートで紹介した4つのテーマはいずれも現在進行形で対応が求められている重要な課題ですが、対策において鍵となるのが"プロアクティブな対応"です。セキュリティソフトや機器のアラートに応じてアクションを起こすリアクティブな対応に加え、本編で触れた"自社の脆弱点を能動的にチェックして修正するサイクルをまわす"、"攻撃元の情報や攻撃手法の変化に連動して防御策を講じる"、"サイバーインテリジェンスを活用してサービス設計や運用に活かす"といった対応を取ることが必須であると言えるでしょう。同時に、限りあるリソースでプロアクティブなセキュリティ対策を業務に取り込む際は、自動化の可能性を検討することも重要となります。パスワードリスト型攻撃のパートでご紹介したクラウドWAFと連動した自動遮断はその一例となります。

今後もセキュリティ対策や情報収集の参考にしていただくべく、Deloitte CICによるセキュリティ監視およびインテリジェンスサービスで得られた知見や分析結果を海外動向と合わせて発信していきます。

デロイト トーマツ サイバー合同会社
Cyber Intelligence Center (CIC)
Mail　ra_info@tohmatsu.co.jp
URL　www.deloitte.com/jp/dtcy
【国内ネットワーク】　東京・名古屋・福岡