F-Secure

2018年上半期
サイバー攻撃の
ランドスケープ

はじめに

2018年上半期のサイバー攻撃の特徴は、過去数年間のトレンドやパターンから変化が見られたことです。

マルウェアに関しては、システムセキュリティの進化とアンチウイルス技術の向上により、ソフトウェアエクスプロイトが削減しコモディティ化された脅威の阻止に成功しましたが、その結果、電子メールスパムが感染ベクター（経路）として復活しました。一方で、企業を恐怖に陥れたランサムウェアは、依然として大きな脅威ではあるもののもはや最大の脅威ではなくなりました。そして、暗号通貨のマイニングの広まりを背景にした新しいトレンドであるCryptojackingが増えています。

エフセキュアのハニーポットネットワークが捕捉した世界的な攻撃トラフィックの傾向として注目されるのは、攻撃トラフィックの発信源として、イギリスがロシアを抜いて1位となったことです。ロシアは2016年に集計を始めて以来最大の攻撃源でしたが、初めて首位の座を明け渡しました。2018年上半期の世界の攻撃総数は、直前の2つの半期よりも少なくなりました。

世界の攻撃トラフィック: ハニーポット

「ハニーポット」は、一般には「罠」や「仕掛け線」を意味します。ここで言うハニーポットは、攻撃者の関心を引くためにわざと目立つように設置された囮（おとり）サーバーのことで、SSH、HTTP、SMBなどの一般的なサービスをエミュレートします。よくできたハニーポットは迷路のようなもので、それと知らずに侵入してきた攻撃者の行動を、水槽の中の魚のように観察することができます。ハニーポットは、現代の攻撃者が使用する手法と標的選択のプロセスに関する情報を収集するための、非常に効果的なツールです。また、マルウェアサンプルやシェルスクリプトを収集するためのソースになることもあります。

ハニーポットは実際での使用を意図したものではないため、ハニーポットへのアクセスは、間違い（ありそうもないことですが、誰かがIPアドレスを打ち間違えたなど）か、攻撃者がネットワークまたはインターネットをスキャンしていて見つけたものと考えることができます。攻撃者はネットをスキャンすることで、公開されていて利用可能なサービスを検出するからです。

インターネット上でのプロービング（探査）アクティビティを観察すると、特定のサービスに対する「需要」がどれほど大きいかに関する情報が得られます。プロービングアクティビティの変化は、しばしばIT業界の世界的なイベントに対応しています。過去にSambaプロトコル（ポート445）への探査の急増を観察しましたが、これはWannaCryやNotPetyaマルウェアで使用されていたEthernalBlueエクスプロイトや、MicrosoftがSQL ServerのLinux版をリリースしたことが原因でした。

攻撃者にハニーポットを「見つけさせ」たら、次のステップはそこにアクセスさせることです。ハニーポットは、提供するサービスに攻撃者がアクセスしやすいように意図的に構成されています。たとえばハニーポットは、推測しやすいパスワードを使用していたり、攻撃者が入力した何回目かのパスワードを受け入れるように設定されていたりします。

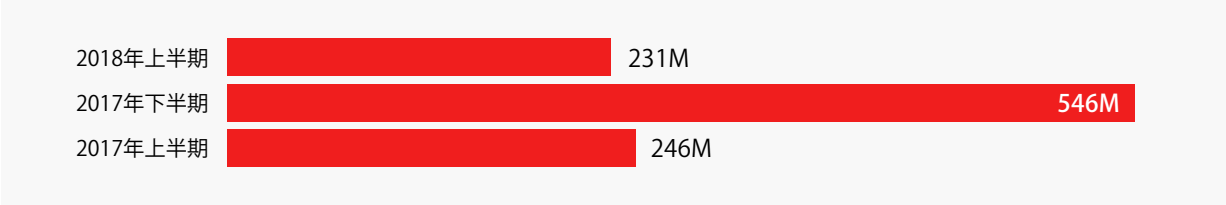
攻撃者がハニーポットへの侵入に成功すると、そこでの行動、接続しようとしている場所、インストールしたマルウェア、ダウンロードするツールなどが記録されます。攻撃者がハニーポットを見つけてから退去するまでの、すべての行動です。

最も効果的なハニーポットは、あたかもそれが特定の目的や組織に役立っているかのように作られており、エリートハッカーを欺くことさえできます。最もよく知られている例の1つは、セキュリティ研究者が自治体の水管理システムをエミュレートするために設定したハニーポットで、中国のハッカー集団（APT1またはComment Crewとして知られている）を捕捉した2013年の例です。

ハニーポットはエフセキュアのRapid Detection & Response Serviceにとって、不可欠な構成要素です。Windows Server、ワークステーション、ファイルサーバー、さらにはVOIPサーバーを模倣するように設計されており、その精度は、ネットワーク通信の下位層でも侵入者を検出することができます。エフセキュアは、お客様環境に加えて、世界中の国々のサーバーで公共のインターネットにハニーポットを展開しています。

このレポートは、ハニーポットで捕捉した国別の攻撃トラフィックを示したものです。データを検討する際には、攻撃の発信源に見える国が必ずしも攻撃の発生場所であるとは限らないことを忘れてはいけません。それは、法的責任を回避するために、複数のプロキシ（踏み台）を経由することがあるためです。攻撃者は、VPN、TOR、侵害されたマシンまたはインフラを経由しているかも知れません。

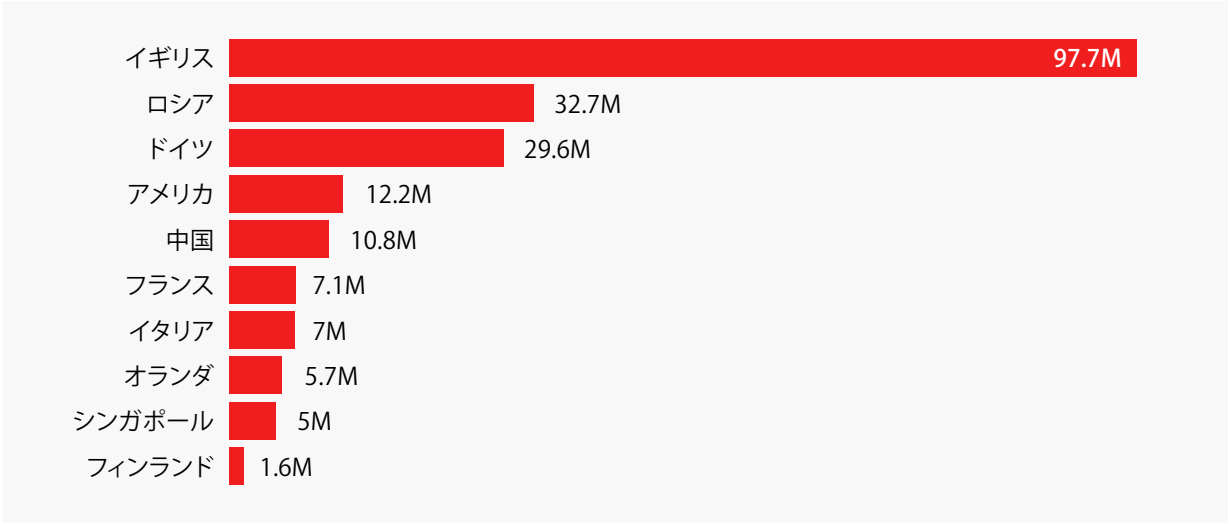
ハニーポットへの攻撃数（グローバル）



2018年の上半期は、直前の半年と比較して攻撃が大幅に減少しました。攻撃トラフィックはSSHプロトコルをターゲットとしたロシアからの大規模な攻撃により、2017年の下半期にピークに達しましたが、今年の第1四半期のロシアのアクティビティは比較的静かで、それが減少の大きな要因となっています。

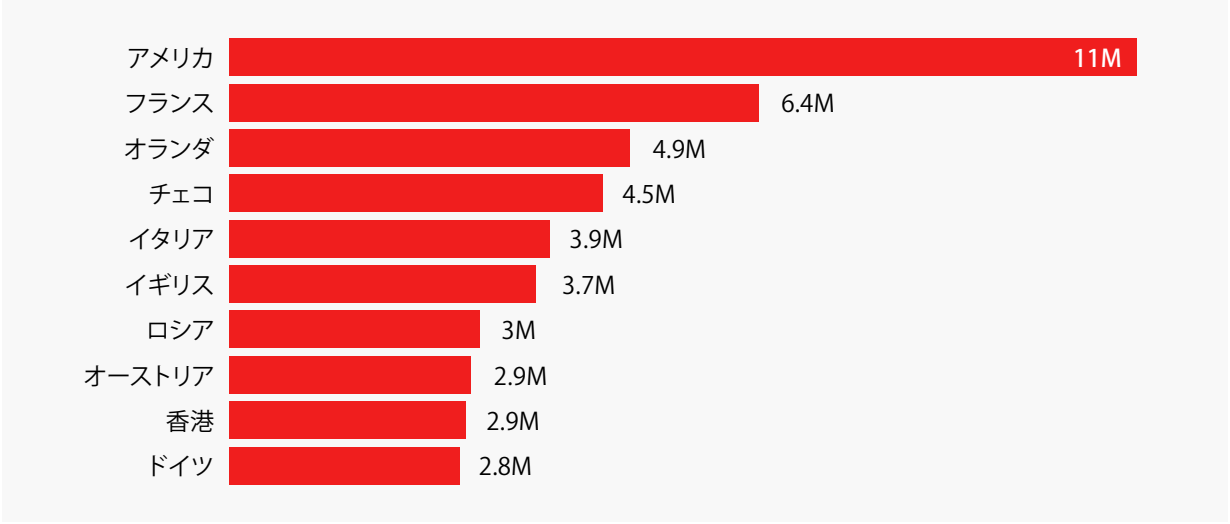
これよりも影響は少ないですが、もう1つの要因はWannaCryが挙げられます。2017年の下半期には、大量のWannaCryに感染したデバイスがSMBポートをプロービングしていました。WannaCryは、未だにエフセキュアのアップストリームテレメトリーで検出されるマルウェアのトップで、これは感染デバイスが潜在的に脆弱なデバイスを見つけるために今もWebをクロールしていることを意味します。しかし、2018年には多くのシステムがアップデートされ、エンドポイント保護ソリューションが感染を阻止しているため、感染デバイスが減少し、上半期にはプロービングアクティビティが少なくなったと考えられます。本レポートではこの後で、ポート445がこの時期に最も多くプロービングされたポートであることに触れますが、そのトラフィックの大半はイギリスからのものでした。これらの攻撃がなければ、445のトラフィックは以前よりも低いレベルでした。

攻撃源となっている国



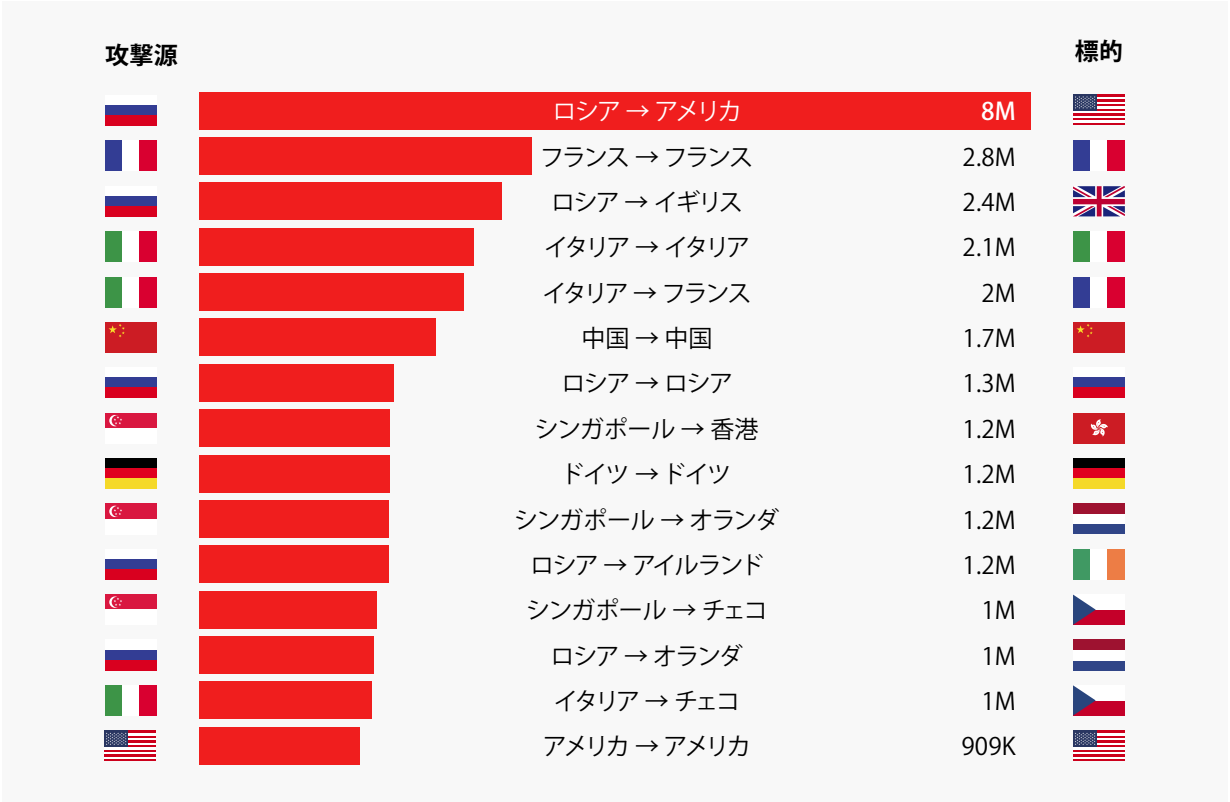
イギリスは今半期を通して活発な攻撃を行い、ロシアを第1位の座から追い落としました。イギリスからのトラフィックの99%がポート445経由でした。フィンランドが初めてリストに掲載されました。ロシアは比較的静かでしたが、これは昨年同期間に1億800万回の攻撃があったのが、3300万回に減ったためです。2017年下半期の攻撃数は1億4,600万回でした。

標的となった国



従来通り、米国は攻撃のトップターゲットでした。ドイツはいつもの5位から10位に下がりました。

誰が誰を狙っているのか: 攻撃源と標的



最も一般的な攻撃源→標的の関係は、ロシアから米国への攻撃です。しかし今回、米国に対するロシアの攻撃数は800万回で、これまでよりもずっと少なくなっています。2016年下半期には、ロシアは米国を標的とした攻撃を約2,700万回行い、2017年上半期は約7,000万回、下半期も約7,000万回の攻撃がありました。

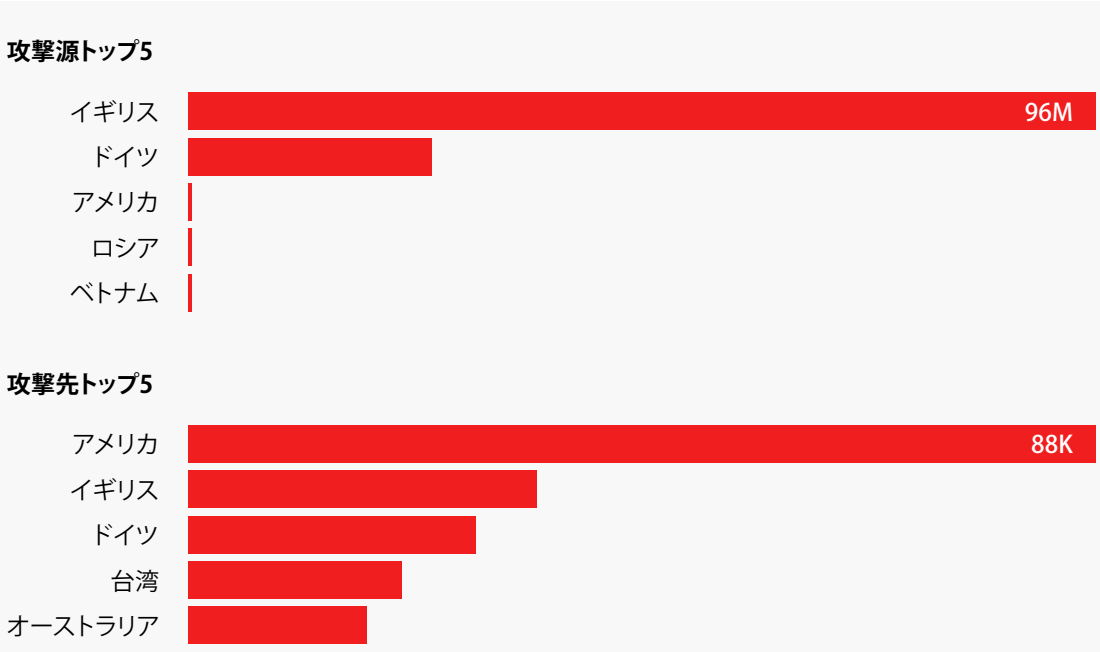
攻撃総数ではイギリスからの攻撃数が最も多かったのですが、このリストでは主要な攻撃源としては表示されていません。それは、標的としている国が多く、標的毎の攻撃数が少なく、最大の標的でもオーストリアで、攻撃件数は39,000件に留まっています。

プロービングされたTCPポート

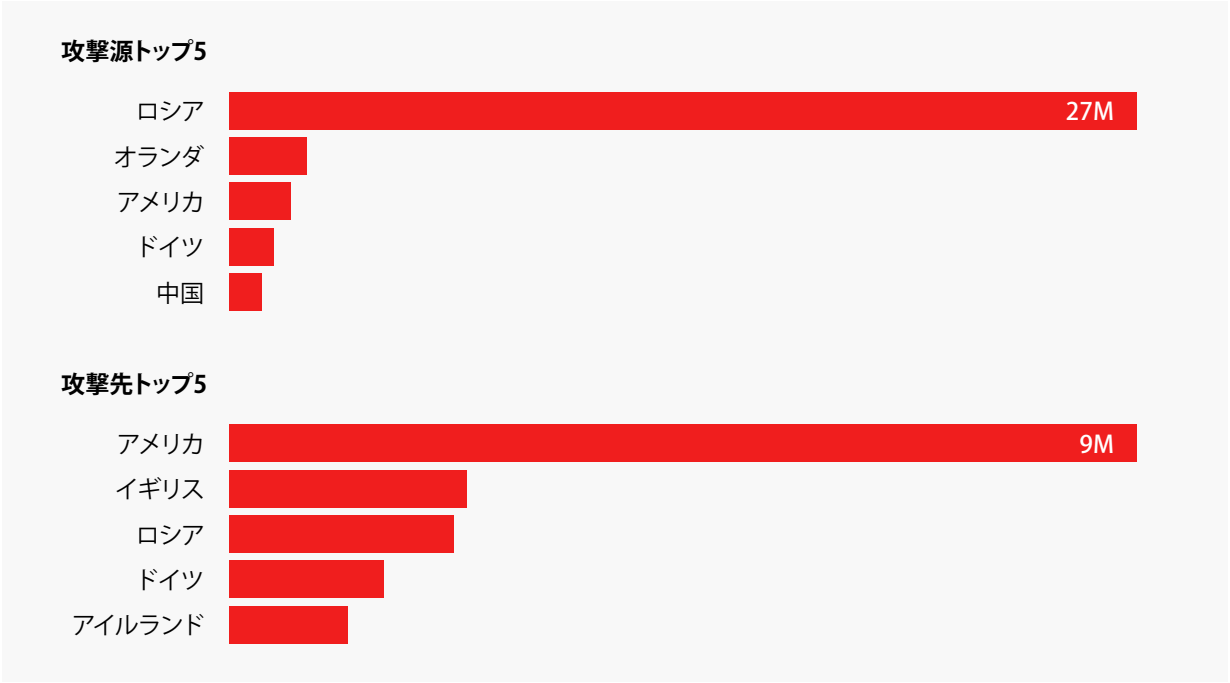
ポート	プロトコル	数
445	SMB	127M
22	SSH	
25	SMTP	
3306	MySQL	
80	HTTP	
1433	MSSQL	
7547	CWMP	
179	BGP	
21	FTP	
8291	Winbox	

このリストでSMBプロトコルがトップになった主な要因は、イギリスからのポート445を狙った活発なアクティビティです。これはEternal Blueエクスプロイトと SMBワームが依然として使われていることを示しているのかもしれません。いくつものタイプのマルウェアが、付加的な感染手法としてこれを採用しています。クリプトミナーといくつかのトロイの木馬がその例で、主にネットワーク上のラテラルムーブメントのためにこの手法を使っています。

SMBアクティビティのブレイクダウン



SSHアクティビティのブレイクダウン



SSHを経由した攻撃は、rootまたはadminとしてログインしようとする試みなどのリモートアクセスの試行を示しています。

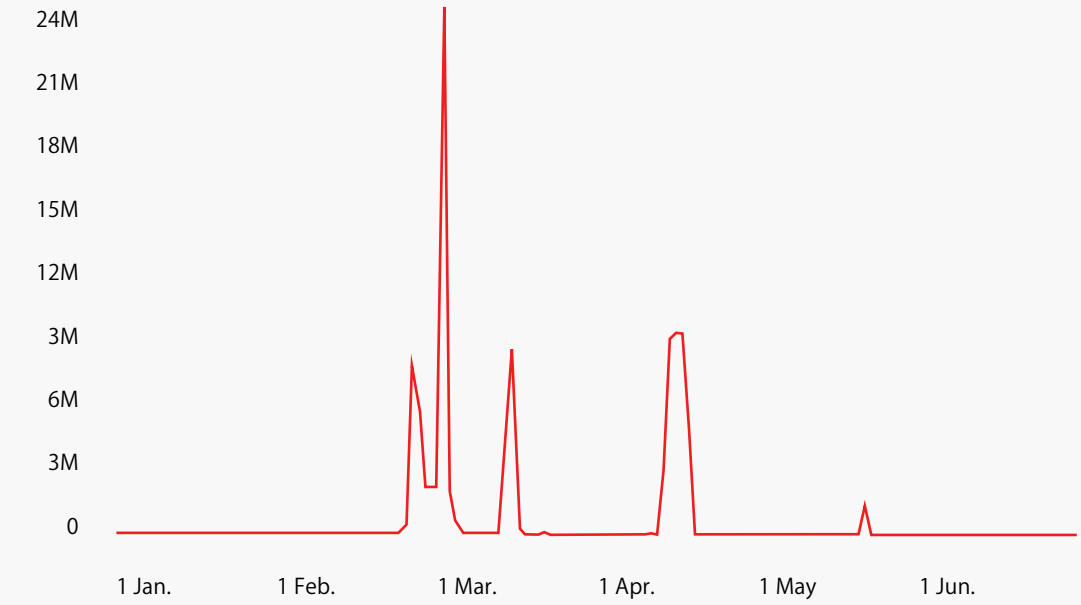
ロシアはSSHトラフィックの発信源として突出していますが、これはいつものことです。

各国の状況

6ヶ月という期間を通じて各国のアクティビティの状況を観察するのは、興味深いことです。いくつかの国で共通に見られたパターンは、1月に活発なアクティビティがあり、その後減少して4月中旬に再びアクティビティが活発化することです。イギリスとデンマークは、このパターンの例外です。

イギリス

以下からわかるように、イギリスはこの期間中に行われた数回の大規模な攻撃によって、1位を獲得しました。攻撃は3月初めに最大となり、約2,400万回のプロービングが行われました。



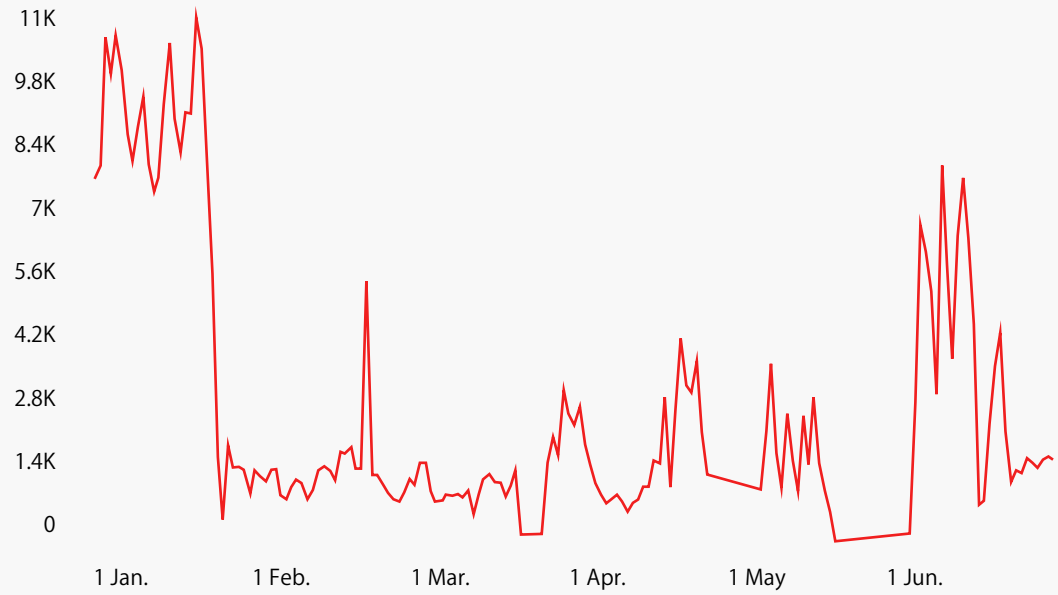
イベント総数: 97,680,746

標的トップ5

最も使われたポート: 445

アメリカ

アメリカからの攻撃が活発化したのは、1月と6月でした。



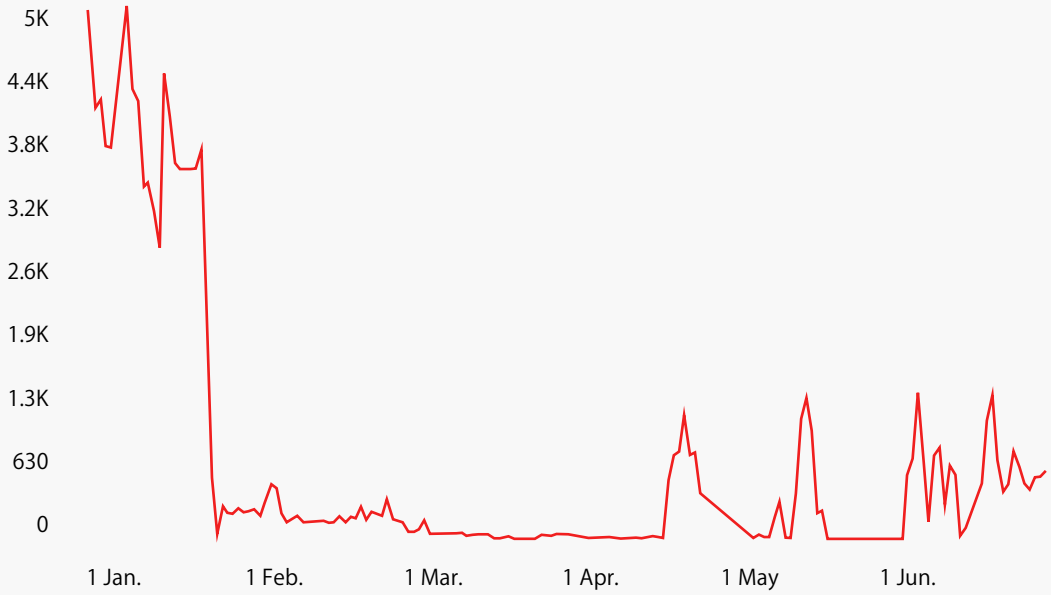
イベント総数: 12,185,768

標的トップ5

最も使われたポート: 22

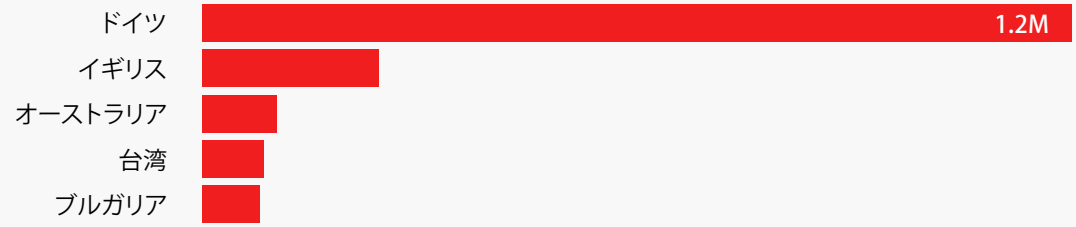
ドイツ

アメリカ同様、ドイツからの攻撃も1月にピークがありました。



イベント総数: 29,574,191

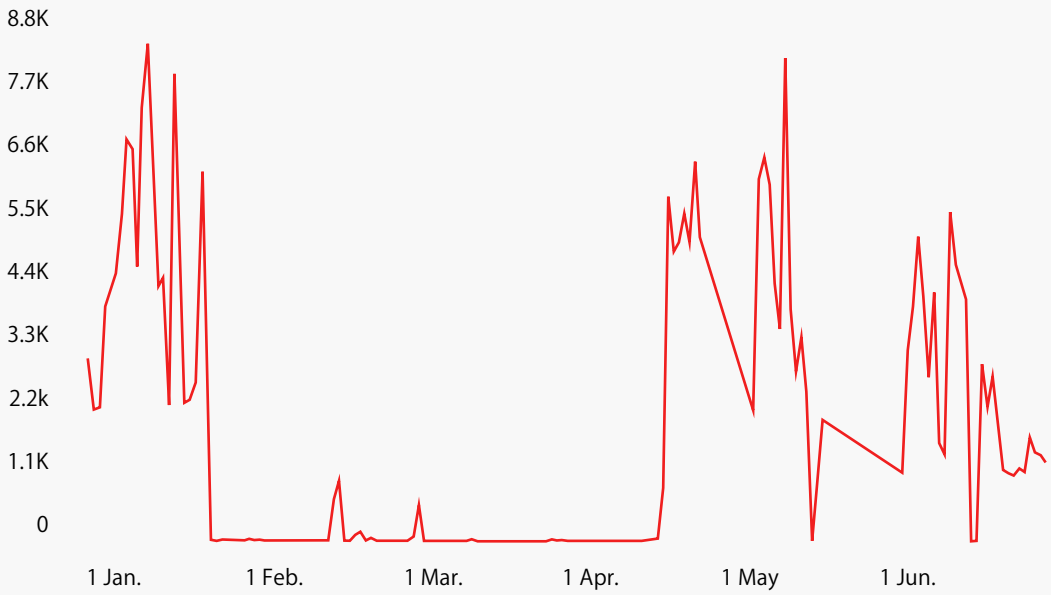
標的トップ5



最も使われたポート: 445

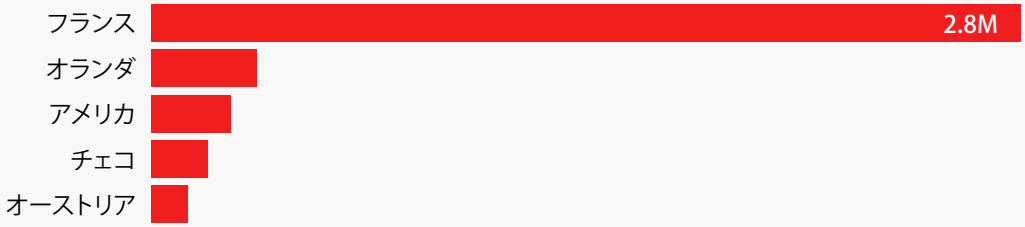
フランス

フランスは、1月と4月中旬以降が最も活発な時期でした。



イベント総数: 7,131,905

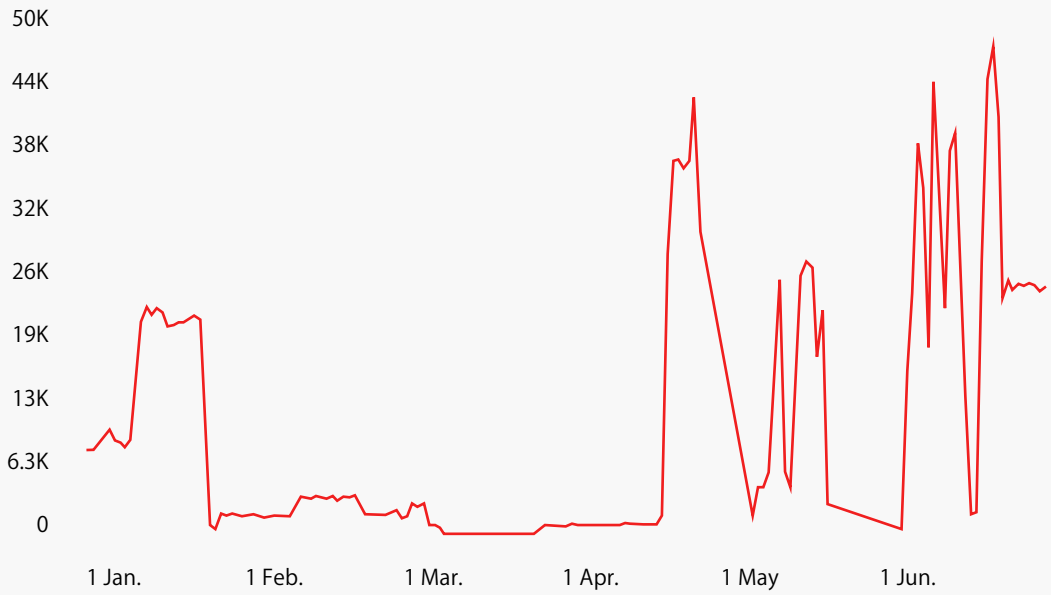
標的トップ5



最も使われたポート: 22

フィンランド

新たにトップ10に入ったフィンランドのパターンは、フランスと似ています。



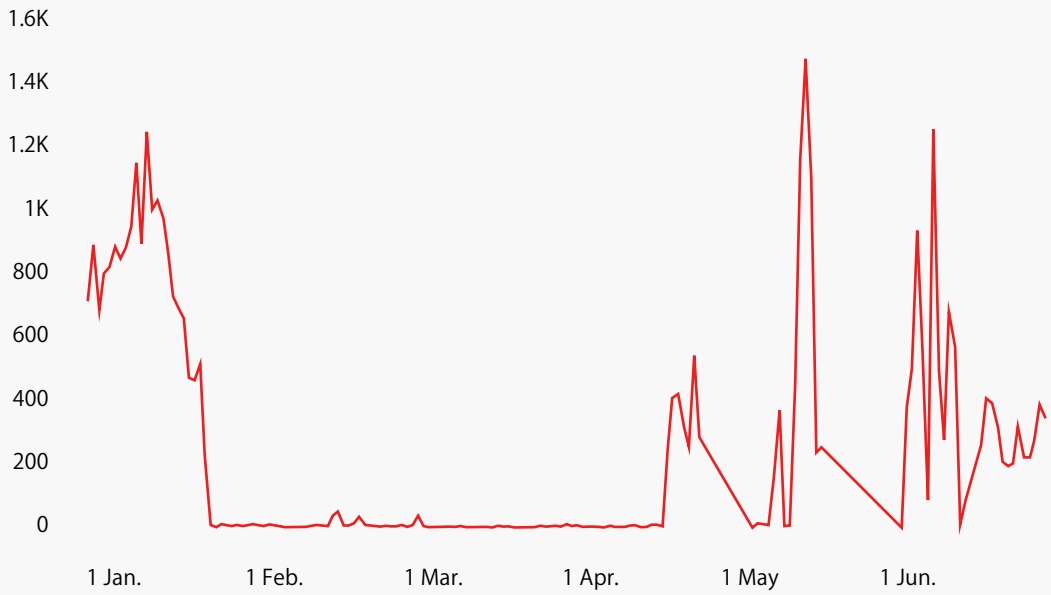
イベント総数: 1,593,790

標的トップ5

最も使われたポート: 22

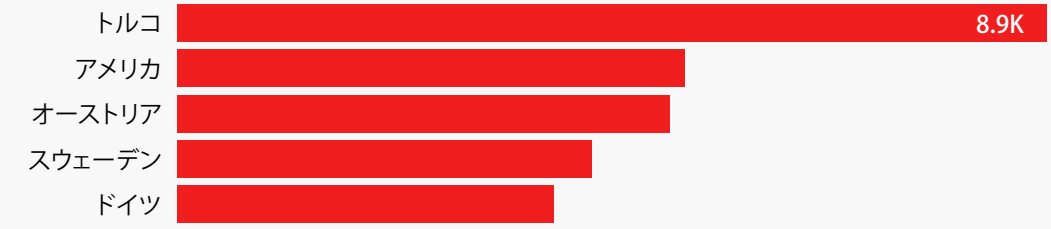
日本

日本のトラフィックも、他の国と同じパターンでした。



イベント総数: 837,873

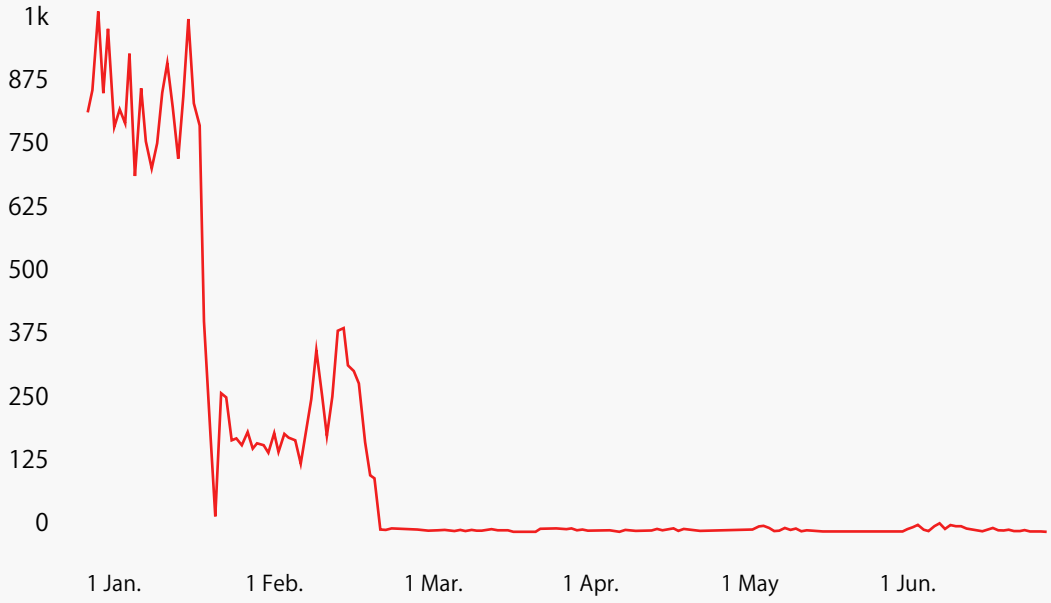
標的トップ5



最も使われたポート: 80

デンマーク

デンマークでも1月にアクティビティが活発化しましたが、他国と違い4月のアクティビティはありませんでした。



イベント総数: 60,9315

標的トップ5

最も使われたポート: 22

お客様環境への最適化

ハニーポットが起動することで、内部に攻撃者が侵入したことを知ることができます。しかし、お客様環境内の攻撃者がハニーポットに触れなかったらどうなるでしょうか? 大量の正規のユーザー行動の海の中で悪意のある行動を見つけ出すことは、乾草の中で針を見つけるようなものになる可能性があります。

前述したRapid Detection & Response Serviceの一環として、エフセキュアは侵害の兆候を検知するのに役立つエンドポイントセンサーをお客様環境内に設置します。

これらのセンサーは、お客様組織全体のコンピュータに設置され、生イベントデータを収集し、バックエンドシステムに転送するように設計されています。人工知能によって強化されたエフセキュアの分析システムによって、異常値として絞り込まれます。異常値はエフセキュアの脅威アナリストによってさらに分析され、フォルスポジティブを除外し、真の脅威は対応方法と共にお客様に報告されます。

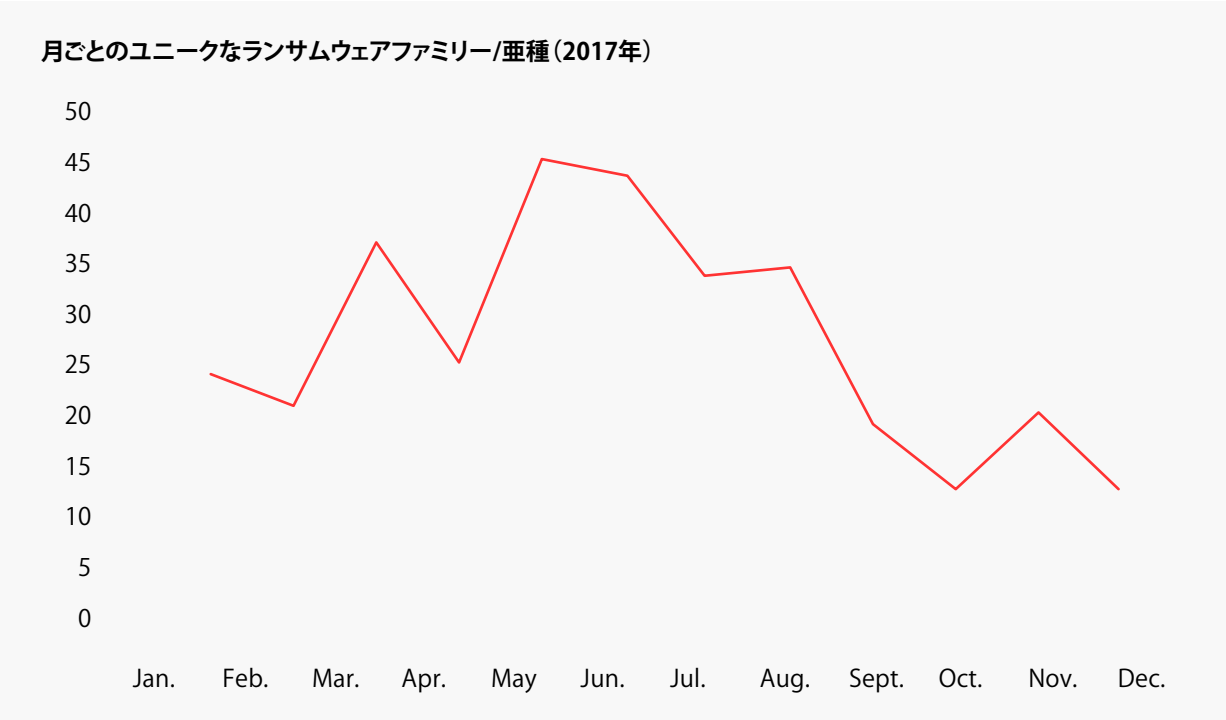
エフセキュアの顧客ベースから収集された生データイベントの数は、半年間で数千億件に達しました。バックエンドのシステムエンジンによる生データ分析の後、数千万件に疑わしいイベントとのフラグが立てられました。

エフセキュアの検出メカニズム、データ分析および脅威アナリストは、これらのうち99.96%を排除し、お客様が数百万のフォルスポジティブに陥るのを防ぎました。最終的に疑わしいイベントのわずか0.004%、つまり顧客ベース全体で数百件が、お客様への真の脅威として特定されました。

個々のお客様には、固有の環境があります。お客様にエフセキュアのレポートから自社の環境について多くのことを学んでいただくため、契約して最初の数カ月間は、意図的に通常よりも多くの異常値を報告します。そうすることで、私たちはお客様と協力して、お客様の特定のネットワーク内でどのような種類の行動が受け入れられ、何が受け入れられないのかを把握することができ、これにより、悪意のある行動をより正確に捉えることができます。

マルウェアのトレンド

今上半期のハイライトは、ランサムウェアの減少とそれを代替する脅威の増加でした。2016年に急増し、組織の最大の脅威となったランサムウェアは、2017年の後半にかけて減少しました。しかし減少したにもかかわらず、今日でも強力な脅威として残っています。



ランサムウェアの減少には、いくつかの要因があります。その1つは、身代金を支払わないようにという啓蒙が進んだこと、そして脅威をどのように予防するかが周知されたことです。「No More Ransom」プロジェクトなどのキャンペーンは、一般の人々の教育に役立っています。さらに、NotPetyaとWannaCryのアウトブレイクの際に、身代金を支払ったにもかかわらずデータを復旧できなかった被害者が続出し、ランサムウェア業界全体が信頼を失いました。2016年の調査「Evaluating the Customer Journey of Crypto-Ransomware」で指摘された、多くのランサムウェア犯罪者が築き上げた評判は失われたのです。

ランサムウェアの減少のもう1つの理由は、ウイルス対策技術が進化し、バルクおよびコモディティ化された脅威を効果的に阻止していることです。最近のスパムメールに添付されているファイルはパスワードで保護されたマクロドキュメントで、パスワードは電子メールの本文に含まれています。この場合、パスワードが使用されるまでファイルが実行されないため、ウイルス対策の検出を回避することができます。しかしこれは、ソーシャルエンジニアリングにおいては最も効果の少ない形態の1つです。マルウェア攻撃がこのようなパスワードで保護された添付ファイルに頼らざるを得ないということは、アンチウィルス技術が有効に機能していることを示しています。

ランサムウェアの減少により、必然的に他のものがその場所を埋めることになり、上半期はそれがCryptojackingとデート詐欺でした。Cryptojackingは、感染したマシンを不正利用して暗号通貨（主にMonero）のマイニングを行うもので、2017年半ばに始まり急速に拡散しました。今ではMimikatzのクレデンシャル取得技術とEternalBlueなどのエクスプロイトを組み合わせ、企業ネットワーク上でのラテラルムーブメント（横展開）を行うマイニングスクリプトも見つかっています。

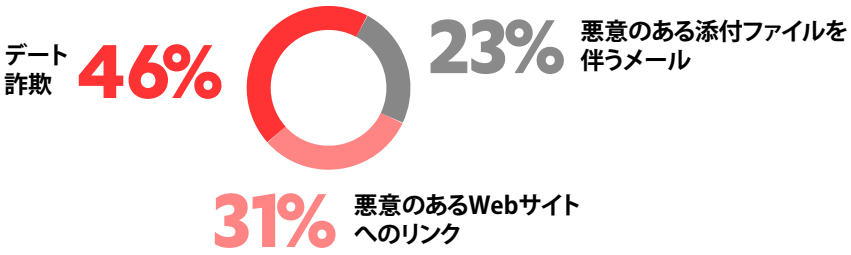
IoTは引き続き、ボットネットの強化を望んでいる攻撃者にとって興味深い対象です。セキュリティが貧弱なLinux IoTデバイスやルーターに感染するLinux TrojanやPNScanなどは、ハニーポットで見つかる最も一般的なマルウェアです。Linuxはデスクトップに広く普及することはありませんでしたが、現在はボットを強化したいと考えるボットマスターが狙う、人気の高いプラットフォームになりました。これは、PCのセキュリティが継続的に強化され、脆弱なPCは既にボットネットに組込まれてしまっているため、新たな犠牲者が必要だからです。

この期間のトップのバンキング脅威（特にスカンジナビアにおいて）は、Trickbotでした。Trickbotは2016年に登場し、新しい機能を追加し続けています。400以上の銀行を含む標的リストには、スカンジナビアの主要銀行のほとんどすべて、そして米国と欧州の主要銀行が含まれています。EternalBlueを使用してパッチ適用されていないWindowsシステムに感染することが知られており、感染後Mimikatzを使用してクレデンシャル情報を取得し、パッチ適用されたシステムに広まります。上半期のある時点で、Trickbotはコインマイニングモジュール XMRigをバックアップの収入源として取り入れました。

スパムは相変わらず強力

悪意のあるURLや添付ファイルを罠として使うスパムは、この期間もトップの感染経路でした。スパムメールの31%は悪意のあるWebサイトへのリンクを、23%は悪質な添付ファイルを含んでいました。マルウェアの添付ファイルの85%が7Z、DOC、PDF、XLSまたはZIPの5つのファイルタイプのうちの1つであることがわかっており、そのほとんどがInfostealer、RAT、およびバンキング型トロイの木馬でした。

残り46%のスパムはほとんどがデート詐欺で、これもどうやら復活してきたようです。これらの電子メールには、独身と思われる個人と連絡を取ることができる電子メールアドレスが含まれており、様々な方法で収益に結びつけようとします。1つの方法は、受信者を有料の出会い系サイトに登録させようとすることです。もう1つもよくある話で、受信者と恋に落ちたようにみせかけ、その上で財政的な「援助」を依頼するものです。

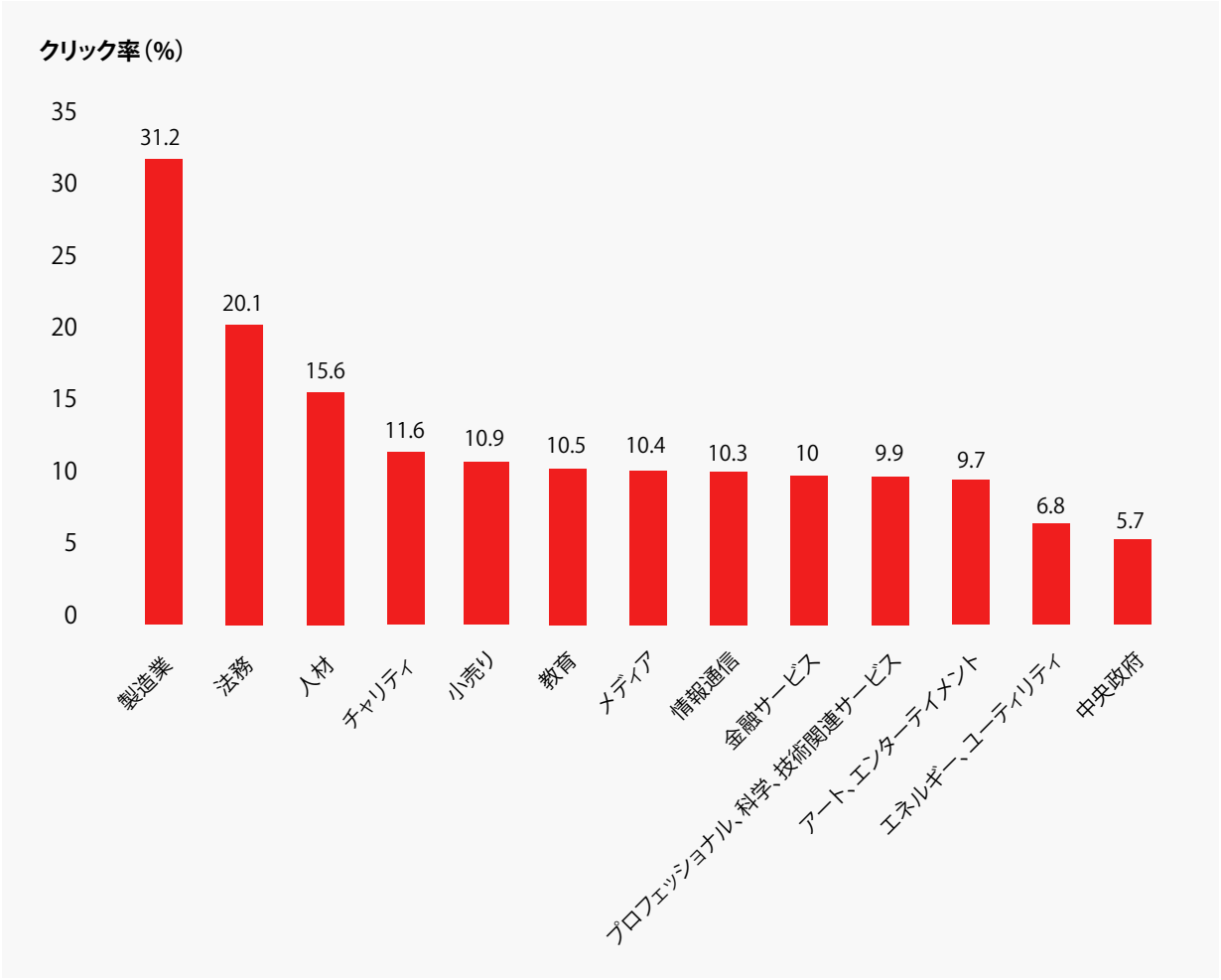


2018年春のスパムサンプル

スパムがますます成功率の高い攻撃経路になっていることは、MWR Infosecurity社のフィッシング評価プラットフォームであるphishdのデータによっても裏付けられています。プラットフォームを通じてクライアントに送信された電子メールのクリック率は、2017年の後半13.4%から2018年の14.2%に増加しました。

スパムの復活は、ソフトウェアの悪用や脆弱性に対抗するためのシステムセキュリティが向上したことが原因です。Flash Playerは、エクスプロイトキットを動かすための最良かつ最後のソフトウェアでしたが、各社のブラウザーが相次いでサポートを停止または縮小しました。こうして経路の選択肢が減ったために犯罪者はスパムに回帰し、その手法とコンテンツを常に改善して人々を騙すための新しい方法を見つけようとしています。今日成功しても翌日同じ手口が通用するかどうかはわからないため、ユーザーを油断させるためには常に変化し続ける必要があります。

また、ユーザーの気を逸らすことも、スパムの有効性を高めます。スパムの危険性は誰もが知っていますが、私たちの注意は常にオンライン上のさまざまなものに向けられるため、最も慎重になるべきクリック行動についての重要性が相対的に低くなります。経営幹部レベルの人物が、他のユーザーと同様にスパム攻撃に引っかかってしまうのは、これが原因です。なぜなら、経営幹部のメール受信箱は常に溢れており、メールを注意深く読むための時間が最も少ないからです。



業種別のスパムクリック率（過去5年間にフィッシング被害に遭ったプラットフォームで収集）

MWR Infosecurity社の研究で、スパムメールのクリック率を左右する興味深い特性が明らかになりました。

既知の送信者からのメール

受信者がスパムをクリックするかどうかに影響を及ぼす最大の要因は、そのメールが知人からのメールであると表示しているかどうかです。知り合いを装ったメールは、クリックされる確率が12%高くなります。

適切な件名がついているメール

信頼できる件名は、スパムが成功するかどうかに大きな役割を果たします。件名に間違いがない場合、電子メールはより正当なものと認知され、スパムの成功率は4.5%向上します。

緊急性を仄めかすメール

あからさまに緊急性を訴えるよりも、単に緊急性が暗示されている場合のほうが、クリックされる確率は1%高くなります。「あなたの注文を完了するために追加情報が必要です。」と、「**今すぐ返信しなければ、注文がキャンセルされます!**」とを比べてみてください。

結論として

サイバーセキュリティにおいて唯一変らない属性は「変化」であり、2018年も例外ではないでしょう。システムセキュリティとユーザー意識を向上させ、欠陥のあるソフトウェアを排除することによってのみ、犠牲者を増やし続けようとする攻撃者の戦術に適応し対応することが期待できます。

闘う相手が、新たなトレンドとして台頭してきたCryptoJackingであっても、デート詐欺やスパムの復活といった古くからのトリックであっても、あるいは攻撃源リストに新たに名を連ねた国々であっても、確実なことが1つあります。それは、コネクテッドワールドのダークサイドとの闘いにおいて、立ち止まっている暇はないと言うことです。

エフセキュアは、他のどの企業よりもサイバーセキュリティを知っています。エフセキュアは30年間に渡ってサイバーセキュリティの革新を主導し、何万もの企業や何百万人もの人々を守ってきました。エフセキュアは、エンドポイント保護と検出とレスポンスにおける卓越した経験を元に、高度なサイバー攻撃やデータ侵害から幅広い脅威に至るまで、企業と消費者を保護します。エフセキュアの洗練されたテクノロジーは、世界的に著名なセキュリティラボの専門知識と機械学習を組み合わせ、ライブセキュリティという高度なアプローチを可能にします。エフセキュアのセキュリティ専門家は、欧州において他のどの企業よりも多くのサイバー犯罪の現場調査に参加しており、その製品は200を超えるブロードバンドおよびモバイル事業者、そして数千社のパートナーによって世界中で販売されています。エフセキュアは1988年に設立され、NASDAQ OMX Helsinki Ltd.に上場しています。

エフセキュア株式会社
〒105-0004 東京都港区新橋2丁目2番9号 KDX新橋ビル2階
Tel: 03-4578-7710 / E-mail : japan@f-secure.co.jp
https://www.f-secure.com/

2018.9 JP